Universidad Austral de Chile

Facultad de Ciencias de la Ingeniería

Escuela de Ingeniería Civil Electrónica

"VULNERABILIDADES DE LAS REDES TCP/IP Y PRINCIPALES MECANISMOS DE SEGURIDAD"

Tesis para optar al título de:
Ingeniero Electrónico.

Profesor Patrocinante:
Sr. Nestor Fierro Morineaud.
Ingeniero Electrónico,
Licenciado en Ciencias de la Ingeniería,
Diplomado en Ciencias de la Ingeniería.

MARCELO ALEJANDRO RIFFO GUTIERREZ

VALDIVIA – CHILE

2009

Comité Evaluador

Profesor Patrocinante :

Néstor Fierro Morineaud

Profesores Informantes :

Pedro Rey Clericus

Raúl Urra Ríos

Agradecimientos

La finalización del trabajo de tesis, es sólo la mínima parte de todo el esfuerzo realizado en los 5 años de estudio y el previo proceso formativo. El esfuerzo real viene de la dedicación, constancia y el cuidado de nuestros cercanos por esmerarse en que seamos personas de bien, recordando siempre dónde crecimos y qué es lo que queremos en la vida en base a los valores adquiridos, que es finalmente lo que permitirá establecer buenas relaciones a lo largo de nuestras vidas.

Es por ello que mis saludos y agradecimientos son especialmente para mi madre María Inés, abuelita Aída, prima Angélica, tío Francisco y mi familia en general, tíos, tías y también para mis amigos que sin considerarse como familia, dentro de la universidad muchas veces pasan a serlo. Un saludo también para mi novia Claudia que es una persona muy importante.

Mi deber sólo fue tener las ganas para lograr mis objetivos, pero sin la ayuda de mis cercanos esto no hubiese sido posible.

Muchas gracias a todos.

Índice

Página

I. Resumen

Capítulo I

En este primer capítulo, quise hacer ver cual es la base que sustenta al modelo TCP/IP, cual es su método de funcionamiento, considerando el soporte que ofrece con sus capas de aplicación, y la jerarquía de operación basada en sus protocolos y servicios. Su análisis, es un factor importante para comenzar a inmiscuirse en las vulnerabilidades de ésta estructura, ya que permitirá saber algunos conceptos que se asociarán a lo largo de la investigación.

Capítulo II

En el Capitulo numero 2 realicé un análisis y mención de algunas de las vulnerabilidades más relevantes que se encuentran presentes en el modelo TCP/IP, mediante ellas se puede tener un concepto más específico de los vacíos o flancos presentes en el modelo, donde terceros pueden obtener algún beneficio o provocar ciertos inconvenientes en el normal funcionamiento. Adicionalmente a estos vacíos con el debido manejo de ciertas variables, herramientas y Software, se puede establecer una manipulación de servicios asociados a la trasmisión, que pueden producir inhabilitación de servicios, ruptura de los datos transmitidos, conflicto de aplicaciones Web, lentitud en la trasmisión de los datos, suplantación de usuarios, suplantación de servicios y manipulación de toda información que esta sujeta a una red, dominio o servidor.

Capítulo III

En el Capitulo número 3 realicé un análisis de la primera barrera de seguridad de la información que circula por la red. Mediante el uso de sistemas de filtrados conocidos como Cortafuegos, se puede dar un grado

de fiabilidad a la información transmitida y así establecer un mejor rendimiento y funcionamiento de la red. Con un buen manejo de los componentes de éstos sistemas, de las arquitecturas, de los sistemas adicionales que presentan, de la amenazas y de las formas de mantener el sistema bajo buenas condiciones de trabajo, se puede comenzar a dar una robustez a los sistemas de prevención y tener un concepto más especifico de la seguridad que necesita una red en particular y así no dejar vacíos que puedan provocar inconvenientes. Sin embargo, se debe estar en un continuo mejoramiento de los sistemas, y considerando las falencias que se presentan. Es importante recalcar que los sistemas Cortafuegos no entregan una respuesta de denegación personalizada, es de tipo genérica de acuerdo a las políticas que se puedan establecer.

En el capitulo número 4, se introducirá un nuevo concepto que permitirá fortalecer la red de los inconvenientes que presentaron en éste capitulo y los cuales no pueden ser resueltos con los sistemas Cortafuegos.

Capítulo IV

De acuerdo con lo mencionado en este capitulo, se realizo un análisis de los mecanismo que permitirán dar una confiabilidad y protección a la red y así establecer una adecuada comunicación, mediante el uso de herramientas que nos permitirán evitar que alguien intercepte, falsifique y manipule los datos que son enviados. Es por ello que la inserción de sistemas criptográficos permitirá seguir elevando el nivel de seguridad y servirá como complemento a los sistemas Cortafuegos que se presentaron en el capitulo anterior. De esta forma la criptografía mediante algoritmos y métodos matemáticos, puede resolver los problemas de autenticidad, privacidad, integridad, no rechazo en la transmisión de la información.

El objetivo final es el envío de información secreta, usando transformaciones en el mensaje, la cuales se conocen como cifrado. El mejoramiento del envío de la información puede ser variable de acuerdo al tipo de cifrado que se utilice, al tipo de sistema criptográfico que este

implementando la Red, el nivel de autenticidad, basado en firmas digitales códigos de envío de mensajes, contraseñas e inserción de protocolos de seguridad a nivel de red y de transporte que permitirán brindar seguridad a una Red. También se debe considerar la inserción de sistemas a nivel de aplicación que son un complemento extra a todos los métodos de seguridad y que pueden entregar una respuesta frente algún inconveniente de violación que se presente. Sumado a ello se detalla la creación de una Red Privada Virtual VPN, que en conjunto con las condiciones mencionadas anteriormente se ira dando una robustez aun mayor.

Capitulo V

En este capitulo se analizo el Protocolo SSH el cual favorece la seguridad en el envío de la información entre dos equipos proporcionando autentificación fuerte, redirección de puertos TCP, sincronización de sistemas de datos, copias de seguridad, comunicaciones seguras sobre canales no seguros entre clientes/servidores bajo una serie de condiciones que favorecen la confidencialidad, autenticación de entidad, autenticación de mensaje y mejorando de esta forma la eficiencia de los sistemas que trabajan con este protocolo.

También se consideraron las principales aplicaciones donde se implementa el protocolo SSH, en conjunto con los protocolos de seguridad nombrados en el capitulo anterior, señalando de esta forma la importancia en el uso de ellos y los alcances de su uso, como pudo ser expuesto al analizar la infraestructura de clave publica (PKI) y la seguridad de transacciones electrónicas (SET) que permiten manejar aspectos complejos de la seguridad bancaria y de la transacciones electrónicas de dinero. Estas mismas condiciones son usadas en otras entidades (Grandes tiendas comerciales, sistemas de compra online, etc), que tienen otros fines, pero que desean proteger de la misma forma la seguridad de los datos que son manejados.

II. Abstract

Chapter I

In this first chapter, my intention was to highlight the base that feeds the TCP/IP model, how it functions, taking into consideration the support that offers with its application layers, and the hierarchy of operation based in its protocols and services.

The analysis of the model is an important factor to start the investigation on the vulnerability of it structure. This will allow knowing some concepts that will be associated along with the research.

Chapter II

In chapter number 2 I analyzed and mentioned some of the most relevant vulnerabilities that are present on the TCP/IP model. Through them, a more specific concept of the shortcomings that are present in the model, in where outsiders or attackers can get a benefit or cause some inconvenient in the regular functioning of it. In addition to these shortcomings , with the proper management of those variables, tools and software, a manipulation of associated services to the transmission can be established, a disruption of the transmitted data, conflict of Web applications, slowness of services and the manipulation of all the information which is connected to a net, domain or server.

Chapter III

In chapter number 3 I analyzed the first bar of security of information that circulates on the net.

Through the use of filtered systems known as firewalls, some degree of reliability of the transmitted information can be given and so to establish a

better performance and functioning of the net. With the proper management of the components of these systems, of operational structures, of the additional systems that present, of the threats and of the ways to keep the system under good conditions of work, a better steadiness of the prevention systems can be given to have a more specific concept of the security that a net in particular needs and therefore to prevent the shortcomings the might cause future inconvenient.

However, regular upgrade of the systems must be done to consider the shortcomings that may appear.

Is it important to take into account that firewalls do not provide a personalized rejection response. It is of generic type according to the policies that can be established.

In chapter number 4, a new concept will be introduced. This will allow to strengthen net from inconvenient that were presented on this chapter and which cannot be solved with the firewall systems.

Chapter IV

According to what was mentioned in this chapter, an analysis of the mechanisms that will allow to provide confidentiality and protection to the net, that way we can establish a right communication, through the use of tools that will avoid someone to intercept, to hack or to manipulate the data that is sent.

That is way the insertion of cryptographic systems will allow the enhancing of the security system and it will be like a complement to the Firewall systems that were presented in the previous chapter. That way, cryptography through algorithms and mathematical methods, can solve authenticity problems, privacy and integrity in the transmission of the information.

The final objective is the sending of secret information, using transformation of the message , which are known as writing in codes. The

development of the sending of information can vary according to the kind of writing of codes that is used, to the type of cryptographic system that is implemented in the net , the level of authenticity, based on the digital signatures, codes of sending of messages, passwords and insertion of security protocols to the net level and to the transport level that will provide security to a net. The insertion of systems to the level of application should be considered as an extra complement to all the security methods and those which can deliver an answer in front of any violation inconvenient that might show up. In addition to that, the creation to a Virtual Private Net VPN is detailed, which along with the previous mentioned conditions, it will give strength to the system.

Chapter V

In this chapter, the SSH protocol was analyzed, this protocol favors the security in the sending of information between two computers allowing strong authentication, redirection of TCP ports, synchronization of data systems, security copies, secure communication about channel that are not safe between client/ servers, under a series of conditions that favor the confidentiality, entity authentication , message authentication. This way it improves the efficiency of the systems that work under this protocol.

The most important application were considered in where the SSH protocol is implemented, along with the security protocols named in the previous chapter. Considering this way the importance in their use and their use.

As exposed in the analysis of the public key infrastructure (PKI) and the security if the electronic transactions (SET) that will allow to take into account complex aspects of the banking security and the electronic transactions of money. These same conditions are used in other entities (big shopping stores, online shopping systems, etc) which have other purposes but that protect the same way as the data that is managed.

III. Introducción

El poder comunicarse es una condición del ser humano que permite interactuar con otros para establecer relaciones, ya sea estas de carácter personal, de negociación y de sincronización.

Esta comunicación con el paso del tiempo ha ido cambiando considerablemente y mas en los últimos 40 años con la creación de los sistemas computacionales, las primeras redes, y principalmente con la Internet que ha permito la mayor evolución y auge en la transferencia y manejo de la información.

De forma conjunta con la evolución en la transferencia de información es que se ha ido desarrollando la forma de proteger esta información que se maneja, y así tener un nivel de seguridad que corresponde de la información.

Es debido a esta constante mejora y desarrollo tecnológico, que he investigado el por qué de algunos inconvenientes que se han presentado en las redes TCP/IP, analizando principalmente aquellos inconvenientes producidos por falencias del modelo TCP/IP, en sus capas y los protocolos que lo sustentan.

Se debe tener considerado que el análisis de estos inconvenientes es fundamental, ya que conociendo donde se encuentran los problemas se puede dar una solución o instaurar métodos de seguridad que permitan tener un resguardo de la información y los datos importantes que se transfieren.

Estas vulnerabilidades son un problema que se debe tener muy bien manejado, debido a que un problema que se presente en el modelo TCP/IP, puede permitir el análisis por parte de personas y una manipulación de la información debido a lo que analice. El análisis por parte de estas personas puede tener fines honestos que permitirán fortalecer la red y fines deshonestos que pueden provocar diversos inconvenientes para su propio beneficio.

Por ello la idea del desarrollo de esta investigación quiere dejar muy en claro cuales son las principales vulnerabilidades usando algunas herramientas y Softwares de búsqueda en base a las vulnerabilidades que serán descritas y que permitirán a terceras personas actuar sobre la red, no profundizando en cuales son las medidas posteriores, es decir, no enfatizando en el ataque en si, sino el las posibles medidas que puede realizar el atacante.

Posteriormente se plantearan las formas o métodos de seguridad más importantes que le darán un grado de confidencialidad, integridad y resguardo a la información que circula por la red, considerando las diferentes condiciones de los equipos que pueden ser utilizados para tal hecho, seguido de los sistemas de claves codificadas y decodificadas en base a algoritmos de cifrado conocido como criptografía.

Finalmente se describirán los principales métodos y protocolo de seguridad que incorporan las mas importantes aplicaciones usadas hoy en día en áreas que necesitan un mayor resguardo de la información que se trasfiere por la red.

IV. Objetivos

Objetivos Generales

- **Identificar las vulnerabilidades de una red TCP/IP.**
- **Identificar la vulnerabilidad en el modelo TCP/IP.**
- **Identificar los diferentes medios de prevención.**
- **Identificar los diferentes medios de protección.**

Objetivos Específicos

- **Ver las principales formas en la que se vulnera un sistema y las consecuencias que provoca en la red.**
- **Analizar los puertos principales donde se identifican las violaciones de la red.**
- **Analizar las vulnerabilidades presenten en los protocolos de comunicación de las capas del modelo TCP/IP.**
- **Ver los problemas ocasionados en la redes por deficiencias de Software.**
- **Analizar los mecanismos de prevención, sus formas de operar, el mantenimiento y las consideraciones que se deben tener en su resguardo.**

- **Analizar los mecanismo de protección, ya sea de encriptación y autenticación de la información.**

- **Mecanismos de protección a nivel de capas del modelo TCP/IP, capa de red, Internet, Transporte y aplicación.**

- **Analizar y ver las vulnerabilidades de la red TCP/IP bajo condiciones de operación y los medios de resguardo frente a situaciones de este tipo.**

CAPITULO I:

Estructura de Funcionamiento Red TCP/IP

1 *MODELO TCP/IP*

Para comenzar a determinar los puntos vulnerables y las medidas de seguridad de una red, es necesario ver su configuración o estructura de funcionamiento. Para esto hay que basarse en el modelo TCP/IP, el cual detalla de forma clara cómo viaja la información a través de la red. Éste modelo es una mejora del modelo de referencia OSI, el cual presenta ciertas falencias de carácter más amplio y una mayor complejidad, por lo tanto, con el modelo TCP/IP se simplificó y replanteó la estructura de cómo la información se traslada a través de la red [15].

Este modelo es la base del Internet que sirve para interconectar equipos computacionales que utilizan diferentes sistemas operativos, teléfonos del tipo IP y todo dispositivo que tenga una Tarjeta de Red, ya sea de forma alámbrica, inalámbrica, de área extensa o de área local.

TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el Departamento de Defensa de los Estados Unidos, ejecutándolo en el ARPANET, una red de área extensa del departamento de defensa.

El modelo TCP/IP forma parte de un protocolo DARPA (Defense Advanced Research Projects Agency), cuyo objetivo era proporcionar y servir con una transmisión fiable de paquetes de datos sobre diferentes redes [2].

El nombre TCP/IP proviene de dos protocolos, los cuales son el Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP), de los cuales se detallaran los principales conceptos asociados a cada término:

1.1 Protocolo de Internet (IP)

Éste protocolo permite a las aplicaciones ejecutarse transparentemente sobre diferentes redes conectadas. Es de esta forma se permite el desarrollo y transporte de datagramas de IP (paquetes de datos), aunque sin garantizar su entrega. Es aquí donde el protocolo IP procesa datagramas IP de manera

independiente sin definir su representación, ruta o envío. Es así como el protocolo IP puede determinar el destinatario del mensaje mediante 3 campos:

- **Campo de dirección IP: Está dada por la dirección del equipo.**

- **Campo de máscara de subred: La cual permite al protocolo IP establecer la parte de la dirección IP que se relaciona con la red.**

- **Campo de pasarela predeterminada: La cual permite al protocolo IP saber a qué equipo enviar un datagrama.**

1.2 Protocolo de Control de Transmisión (TCP)

Es un protocolo que asegura que los datos sean recibidos de la misma forma que fueron enviados, estableciendo una comunicación entre 2 o más equipos, por lo tanto, es un protocolo orientado a la conexión que permite la unión de dos equipos, en donde existe un cliente y un servidor que responde a las solicitudes generadas de forma simultánea. El protocolo TCP en conjunto con los equipos de soporte, se encargan de manejar la velocidad de los mensajes emitidos, debido a la capacidad que tiene de manipular los mensajes en diferentes tamaños (segmentos).

Las principales características del protocolo TCP son las siguientes:

- **Permite colocar los datagramas nuevamente en orden cuando vienen del protocolo IP.**

- **Permite el monitoreo del flujo de los datos para así evitar la saturación de la red.**

- **Permite que los datos se formen en segmentos de longitud variada para entregarlos al protocolo IP.**

- **Permite multiplexar los datos, es decir, permite que la información que viene de diferentes fuentes pueda ser transmitida en una misma línea (circulación simultáneamente).**

- **Permite comenzar y finalizar la comunicación amablemente.**

Bajo su funcionamiento, se transfieren datos mediante el ensamblaje de bloques de datos conocidos como paquetes. Cada paquete comienza con una cabecera que contiene información de control y validación, seguido de los datos.

Cuando se envía un archivo por la red TCP/IP, su contenido se envía utilizando una serie de diferentes paquetes. Es así como se establece la forma de operación general bajo estos dos protocolos.

Debido a lo mencionado anteriormente, se puede señalar que éste modelo es fundamental para comenzar el análisis de los puntos defectuosos de la red [6]**. En la figura N° 1.1 se puede apreciar la configuración del modelo.**

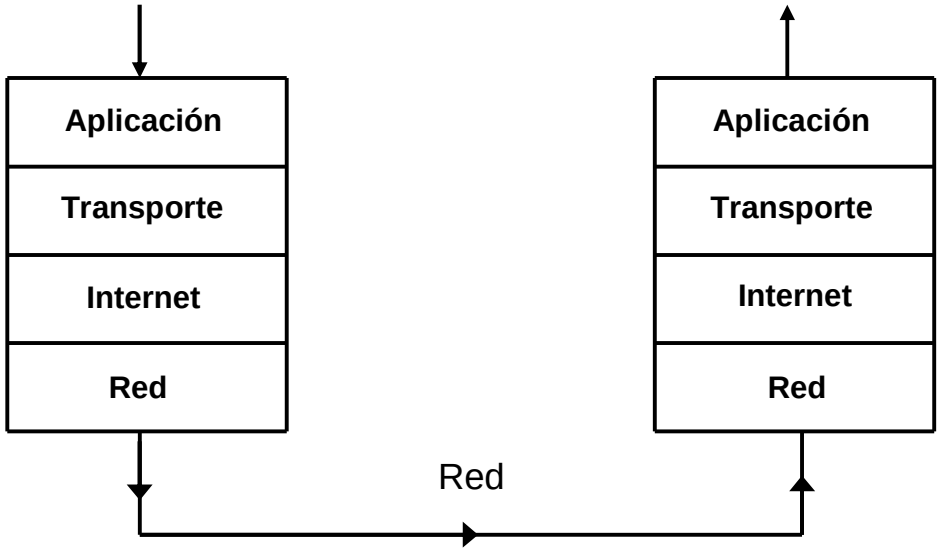


Figura N°1.1 – Modelo TCP/IP

Es así como ésta estructura o modelo representa la forma en que la información circula por la red, donde cada etapa le da soporte a la capa superior, y así posteriormente a la familia de protocolos TCP/IP que necesita para establecer la comunicación.

1.3 Etapas del Modelo TCP/IP

A Continuación se mencionarán las principales funciones de cada etapa del modelo TCP/IP:

Capa de Red : La Capa de Red es responsable de aceptar los datagramas IP y transmitirlos hacia una red específica. Éstos datagramas IP forman parte del paquete y sirven para realizar un mejor encaminamiento o ruteo de los datos permitiendo que lleguen a destino.

Una interfaz de red puede consistir en un dispositivo controlador (Ej: cuando ésta es una red de área local a la que las máquinas están conectadas

directamente) ó un complejo subsistema que utiliza un protocolo de enlace de datos propios.

Capa de Internet : La Capa de Internet maneja la comunicación de una máquina a otra. Ésta acepta una solicitud para enviar un paquete con la identificación de la máquina hacia la que se debe enviar el paquete. La capa de Internet también maneja la entrada de datagramas, verifica su validez y utiliza un algoritmo de ruteo para decidir si el datagrama debe procesarse de manera local o debe ser transmitido. Para el caso de los datagramas direccionados hacia la máquina local, el Software de la capa de red de redes borra el encabezado del datagrama y selecciona, de entre los varios Protocolos de Transporte, un protocolo con el que manejará el paquete. Por último, la capa Internet envía los mensajes ICMP (Protocolo de Control de Mensajes de Internet) de error y control necesarios y maneja todos los mensajes ICMP entrantes. Ésta capa permite que todos los puntos de la red se puedan interconectar mediante un direccionamiento o encaminamiento de lo paquetes de datos.

Capa de Transporte : La principal tarea de la Capa de Transporte es proporcionar la comunicación entre un programa de aplicación y otro. Éste tipo de comunicación se conoce frecuentemente como comunicación punto a punto. La capa de transporte regula el flujo de información. Puede también proporcionar un transporte confiable, asegurando que los datos lleguen sin errores y en secuencia. Para hacer esto, el Software de Protocolo de Transporte tiene el lado de recepción, enviando acuses de recibo de retorno y la parte de envío retransmitiendo los paquetes perdidos. El Software de transporte divide el flujo de datos que se está enviando en paquetes (pequeños fragmentos del mensaje) y pasa cada paquete, con una dirección de destino hacia la siguiente capa de transmisión. La Capa de Transporte debe aceptar datos desde varios programas de usuario y enviarlos a la capa del siguiente nivel. Para hacer esto, se añade información

adicional a cada paquete, incluyendo códigos que identifican qué programa de aplicación envía y qué programa debe recibir, así como una suma de verificación para chequear que el paquete ha llegado intacto y utiliza el código de destino para identificar el programa de aplicación en el que se debe entregar. La Capa de Transporte está encargada de dar el grado de fiabilidad de información que circula por la red, es decir, que la información llegue a destino mediante un control de flujo y de errores. Pero, no se encarga de realizar una verificación si los datos fueron recepcionados.

Capa de Aplicación : Es el nivel más alto, aquí los usuarios llaman a una aplicación que acceda servicios disponibles a través de la red. Una aplicación interactúa con uno de los protocolos de nivel de transporte para enviar o recibir datos. Cada programa de aplicación selecciona el tipo de transporte necesario, el cual puede ser una secuencia de mensajes individuales o un flujo continúo de octetos. El programa de aplicación pasa los datos en la forma requerida hacia el nivel de transporte para su entrega. Esta capa permite al usuario disponer de los servicios que ofrece la red, tales como correos, servidores Web entre otros.

Continuando con el proceso de identificación de los principales conceptos asociados al modelo TCP/IP, se presenta un aspecto que le da soporte y flexibilidad a la red, el cual es su familia de protocolos. Bajo su estructura hace posible la comunicación entre capas y posteriormente entre diferentes usuarios.

1.4 Familia de Protocolos Modelo TCP/IP

En la figura N° 1.2 se puede apreciar la forma como opera esta familia de protocolos:

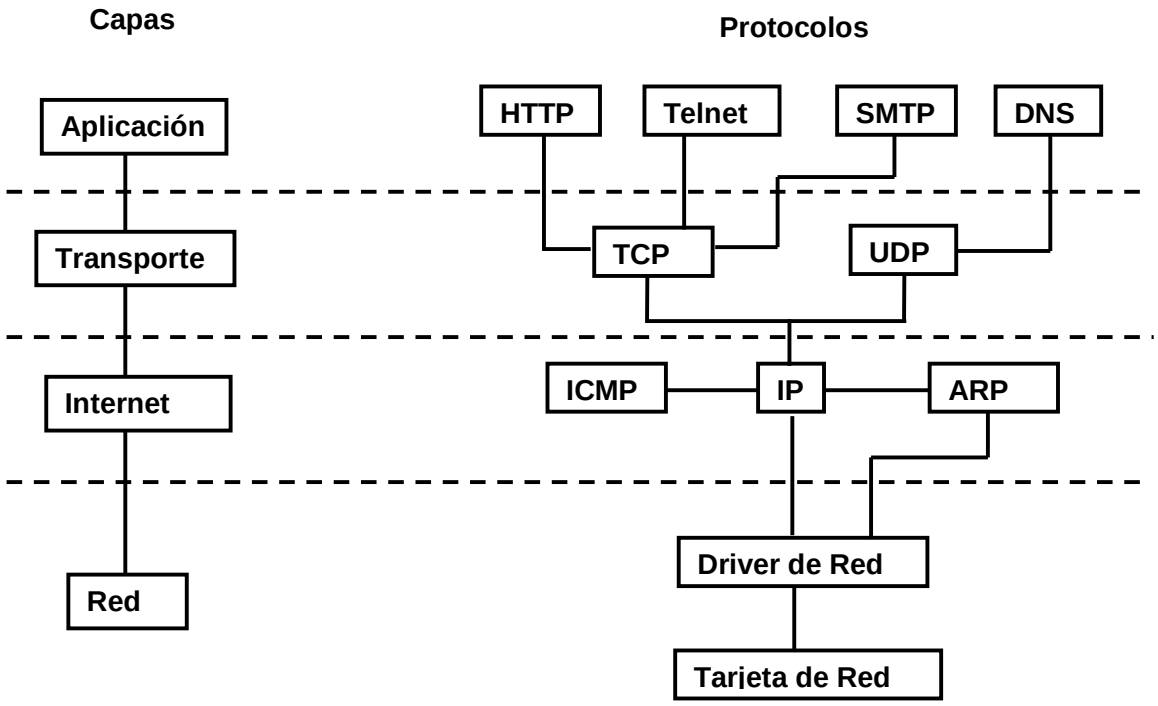


Figura N° 1.2 – Capas y Respectivos Protocolos Modelos TCP/IP

Esta disposición y estructura son parte fundamental del análisis que realizo [6]**, ya que es aquí donde se producen los principales conflictos y vulnerabilidades.**

Es por ello que a continuación se detallarán las principales funciones de cada protocolo y sistemas necesarios para establecer la comunicación que se apreciaron en la figura número 2:

Tarjeta de Red : La Tarjeta de red, también conocida como Tarjeta de Interfaz de Red (NIC), es un Hardware necesario para poder establecer una comunicación entre 2 o más equipos [13]**.**

Una tarjeta de red, convierte los datos enviados por un equipo a un formato que pueda ser utilizado por el cable de red, transfiere los datos a otro equipo y controla a su vez el flujo de datos entre el equipo y los cables conectores (RJ45). Se encarga de traducir los datos que ingresan por el cable a la unidad conocida bytes para que el CPU del equipo pueda leerlos. La función de la tarjeta de red es la de preparar, enviar y controlar los datos en la red. Esta tarjeta de red puede ser orientada para una conexión física o de tipo inalámbrica.

Driver de Red : El Driver de Red es un Software que sirve de intermediario entre un dispositivo (Hardware) y el sistema operativo que tiene el equipo. Su funcionamiento en el Modelo TCP/IP está basado en permitir una sincronización a través de Software entre el Protocolo IP y la Tarjeta de Red.

Protocolo ARP : El Protocolo de Resolución de Dirección (ARP) permite que se conozca la dirección física de una Tarjeta de Interfaz de Red por medio de una dirección IP y los Driver de Red [6].

Protocolo ICMP : El Protocolo de Control de Mensajes de Internet (ICMP) se encarga de realizar un control de flujo de datagramas IP que circulan por la Red, es decir, se encarga de realizar las notificaciones de posibles errores y de situaciones anormales que se presenten en el envío o recepción de información a través del protocolo IP [6]**.**

Protocolo UDP : El Protocolo de Datagramas de Usuario (UDP) es el que permite crear una interfaz en las aplicaciones IP existentes, es una forma de multiplexar y demultiplexar los datagramas IP enviados a través de la red.

Protocolo HTTP : El Protocolo de Transferencia de Hyper Texto (HTTP) está orientado en permitir la transferencia de archivos en lenguaje de marcación de Hyper Texto (HTML) entre un navegador (el cliente) y un servidor Web localizado mediante una cadena de caracteres denominados dirección de Localización Uniforme de Recursos (URL). Este protocolo se encarga de, en una pagina Web, proyectar los elementos de texto, imágenes, enlaces, inserciones multimedia de audio, entre otros. Al tener un buen manejo de este protocolo, se permite tener un entorno más ameno y agradable a los usuarios.

Protocolo Telnet : El Protocolo de Comunicaciones de red (Telnet) es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos (del lado del servidor). Actualmente, éste protocolo ha evolucionado a un sistema más seguro conocido como SSH (interprete de órdenes seguras).

Protocolo SMTP : El Protocolo Simple de Transferencia de Correo (SMTP) es el que permite la transferencia en línea de correos desde un servidor a otro mediante una conexión punto a punto.

DNS : Es un Servidor de Dominio de nombres de servicios que permite traducir de nombre de dominio a dirección IP. De ésta forma, DNS seria una base de datos, en donde se encuentran las direcciones necesarias solicitadas por los usuarios para establecer sus peticiones de conexión en un servidor determinado [4]**.**

CAPITULO II:

Deficiencias de la

Red TCP/IP

1 *ASPECTOS GENERALES DE VULNERABILIDAD EN MODELO TCP/IP*

Este capítulo quiere dar a conocer cuales son las vulnerabilidades que se producen en el modelo TCP/IP, identificando los principales inconvenientes de cada etapa y de los protocolos.

El objetivo es determinar bajo éstos problemas, la forma en que terceras personas (atacantes) burlan a los usuarios que se manejan en una red determinada, ya sea interrumpiendo la comunicación, deshabilitando servicios, manipulando información y produciendo conflictos en los sistemas con los que trabajan, entre otros aspectos.

Es importante recalcar que el acceso a cada etapa estará determinado por el grado de fiabilidad que brinda la misma red, por ello, si un intruso tuviera el acceso a ésta, puede sin ningún problema examinar cada protocolo para encontrar los puntos de inflexión de la red y obviamente en base a ello, ocasionar algún problema.

1.1 Vulnerabilidades en capas de modelo TCP/IP

En base al modelo TCP/IP se puede realizar un enfoque general de vulnerabilidad de cada etapa, las cuales se detallan a continuación:

1.1.1 *Capa de red*

Los principales inconvenientes en esta capa pueden ocurrir si alguien tuviera acceso a los equipos con los que la red opera, es decir, acceso al cuarto de telecomunicaciones, al cableado o a los equipos remotos establecidos para la comunicación (ataques realizados en la capa de red pueden ser los que ocurren en líneas de cableado, desvío de cableado, interceptación de comunicación entre equipos), es por ello que los principales inconvenientes que pudiesen presentarse en esta capa, están

asociados al grado de confidencialidad y control de acceso que pueda tener o manejar una persona.

A continuación se mencionarán las tres condiciones esenciales que tiene esta capa que deben ser resguardadas, ya que con una mala manipulación puede perjudicar a una Red o a un usuario particular:

La Confidencialidad : Es la privacidad que posee cualquier documento enviado por la red o mecanismos que necesiten un control de acceso, es así que se debe garantizar que éstos estarán disponibles únicamente para la persona autorizada a acceder a dicha información.

Autenticidad : La autenticación es el proceso de verificación de identidad digital en una comunicación que permitirá conocer la validez de los usuarios y datos que se manipulan.

Integridad : Es la garantía de la exactitud de la información frente a la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta, refiriéndose principalmente a la fidelidad de la información que debe mantenerse entre el emisor y el receptor.

En los siguiente ítemes y a un nivel más específico, los problemas se asocian a la interceptación de información (ítem 2.2), la suplantación de mensajes y direcciones IP, los que se generan tras alterar el funcionamiento del Control de Acceso al Medio (ítem 2.2.1) y aprovechar las falencias físicas que presentan en la Tarjeta de Interfaz de Red, burlando éstas tres condiciones esenciales que debe brindar toda red de forma óptima.

1.1.2 *Capa de Internet*

Es la capa de donde mayor información se puede obtener para vulnerar un sistema. Lo fundamental para acceder a ésta es tener acceso a

los datagramas IP los que se pueden encontrar en cada paquete que circula por la red, mediante Softwares espías. Estos Softwares permiten recolectar información mediante un proceso que se conoce como Sniffing, el cual es un término asociado a la captura de información que circula por la red, en donde se puede hacer una separación de la información, para discriminar si es relevante.

Un factor que juega a favor de la persona que desee atacar a un usuario o máquina determinada, está dado por el nivel de autenticación que presenta la capa de Internet, la cual es a nivel de máquina, es decir la IP es asignada por ésta. De ésta forma, si un sistema llegara a presentar una falla, como una dirección incorrecta, el receptor no identificará si esa es realmente la dirección o si es una dirección adulterada por un atacante. Es ése el punto que permite a un atacante tener acceso a esa máquina en particular, pudiendo adulterar su funcionamiento o extraer información. El método más común para acceder a ello, es la predicción de secuencia TCP. Este método hace una simulación de participación en una red, permitiendo tener acceso a una red en particular y lograr robar una sesión TCP. Existen Softwares especializados que se encargan de hacer éstas simulaciones. Otro método es el envenenamiento de tablas caché, que permite suplantar la MAC (Control de Acceso al Medio) y de ésta forma tener acceso a la información que recibe una máquina en particular [14]**. Todos éstos ataques son realizados mediante Softwares espías de tráfico de paquetes de datos, los cuales son de fácil acceso y se encuentran en la red, tales como Caín & Abel, XArp 2, CaptureNet, PeepNet y de los cuales en los siguientes apartados se analizaran los principales Softwares.**

1.1.3 ***Capa de Transporte***

Las principales vulnerabilidades están asociadas a la autenticación de integración y autenticación de confidencialidad [1]**. Estos términos se**

relacionan con el acceso a los protocolos de comunicación entre capas, permitiendo la denegación o manipulación de ellos, los que serán detallados a lo largo del ítems 2.1.3.

1.1.4 *Capa de Aplicación*

Los posibles inconvenientes a presentarse pueden ser ocasionados por cuatro puntos, principalmente los que están asociados a la autenticación de datos y los protocolos presentes en ésta capa.

Punto 1 : Se establecen las deficiencias del servicio de nombres de dominio. Lo que ocurre con éste servicio, es que se encarga de generar las solicitudes de cada usuario que circulan por la red, es decir, en el momento que una persona solicita una conexión a un servicio determinado, se solicita una dirección IP y un nombre de dominio, se envía un paquete UDP (Protocolo de Comunicación el cual envía los datos del usuario) a un servidor DNS (Dominio de Nombre de Servicio). Lo que hace el servidor DNS es responder a ésta solicitud y entregar los datos que fueron pedidos, donde éste servidor DNS funciona como una base de datos en donde se encuentran las direcciones que solicitan los usuarios, por lo tanto, cuando se tiene acceso a esta especie de base de datos se presenta un inconveniente, el cual hace vulnerable al sistema, ya que puede ser modificada a gusto de la persona que le quiere sacar provecho a esa información, pudiendo entregar direcciones incorrectas o recepcionar las peticiones de los usuarios para obtener información acerca de sus cuentas [4]**.**

Punto 2 : Está dado por el servicio Telnet, el cual se encarga de autentificar la solicitud de usuario, de nombre y contraseña que se trasmiten por la red, tanto por el canal de datos como por el canal de comandos.

Punto 3 **: Está dado por File Transfer Protocol (FTP), el cual al igual que el servicio Telnet, se encarga de autentificar. La diferencia se encuentra en que el FTP lo hace más vulnerable ya que es de carácter anónimo.**

Punto 4 **: Está dado por el protocolo HTTP, el cual es responsable del servicio World Wide Web. La principal vulnerabilidad de este protocolo, está asociado a las deficiencias de programación que puede presentar un link determinado** [7]**, lo cual puede poner en serio riesgo el equipo que soporta este link, es decir, el computador servidor.**

2 *VULNERABILIDADES ESPECÍFICAS EN EL PROCESO DE COMUNICACIÓN EN MODELO TCP/IP*

2.1 Identificación de puntos vulnerables en base a la búsqueda de información.

Para determinar qué sistema es más vulnerable, es necesario conocer primero qué es lo que se desea obtener, es decir, el objetivo del ataque que se desea realizar. Para ello en una primera instancia, se debe realizar un proceso de recolección y obtención de información, discriminando que información es más relevante y sencilla de interpretar.

Éste proceso da paso a una serie de posibles formas de obtener esta información, las cuales pueden ir desde las herramientas de administración que poseen los sistemas operativos, hasta sistemas con un mayor grado de especialización, los que se detallarán dentro de los conceptos asociados al ataque.

2.1.1 *Utilización de herramientas de administración.*

Para poder realizar el proceso de recolección, usando las herramientas de administración que ofrecen los sistemas operativos, debemos acceder a los sistemas de comandos y luego realizar ejecuciones de herramientas que puedan dar alguna información del sistema. Entre las principales herramientas o comandos existentes se encuentran: Ping, Tracert, Whois, Finger, Rusers, Nslookup, Rcpinfo, Telnet, Dig, IPConfig, IPConfig/All entre otros (El uso de éstos comandos es realizado bajo la ejecución de CMD en el sistema operativo u/o opción de MS-DOS) [27]**.**

Al usar el comando IPConfig en un equipo, se puede observar la dirección IP asociada al equipo, la dirección IP del adaptador asociada a dicho equipo, el cual permitirá realizar una discriminación en base a prueba y error de las direcciones que estén siendo utilizadas y las que no.

En la figura se puede apreciar el uso del comando IPConfig, bajo la ejecución de CMD:

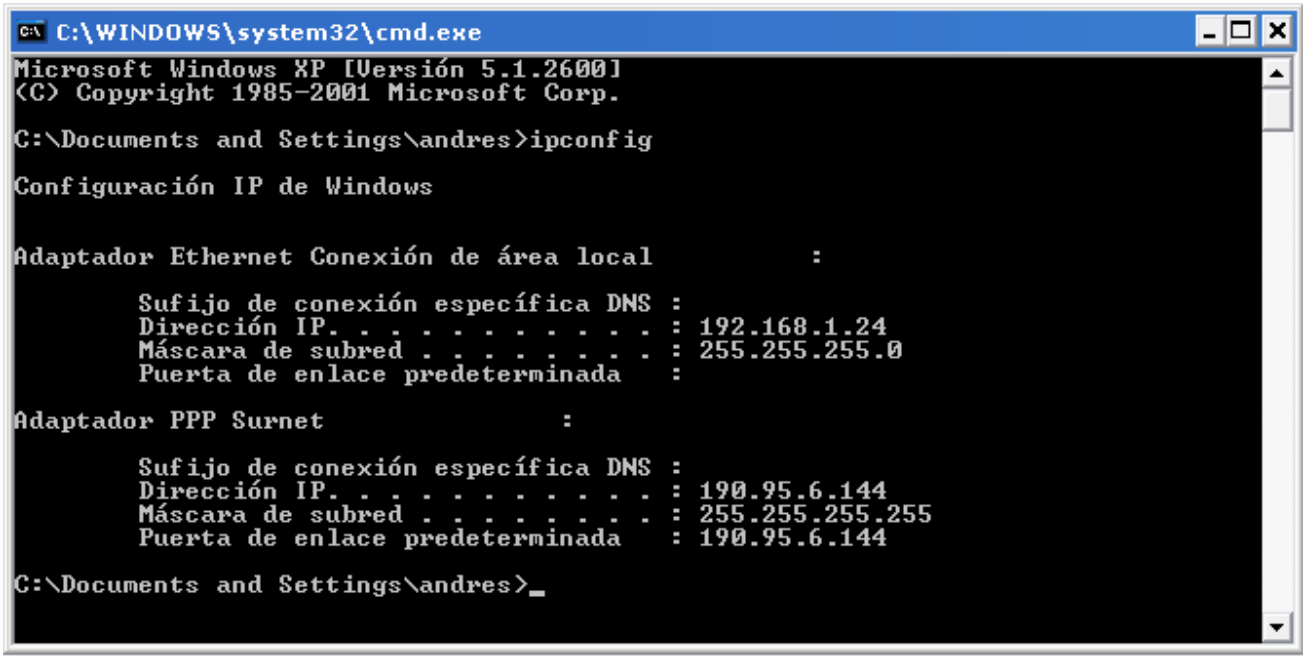


Figura N° 2.1 – Comando IPConfig

Luego de tener éstos datos, se pueden comenzar a realizar pruebas de verificación de las direcciones disponibles usando el Comando Ping. Como se pudo apreciar, la dirección asociada al adaptador es 190.95.6.144, por lo tanto, al usar otra dirección cercana a esta dirección se puede ir verificando si existe algún equipo asociado al adaptador.

Primero se prueba con la dirección 190.95.26.100 con la opción –n (donde n es el número de consultas realizadas, con n=5), del comando Ping y en la figura N°2.2 se puede ver lo acontecido:

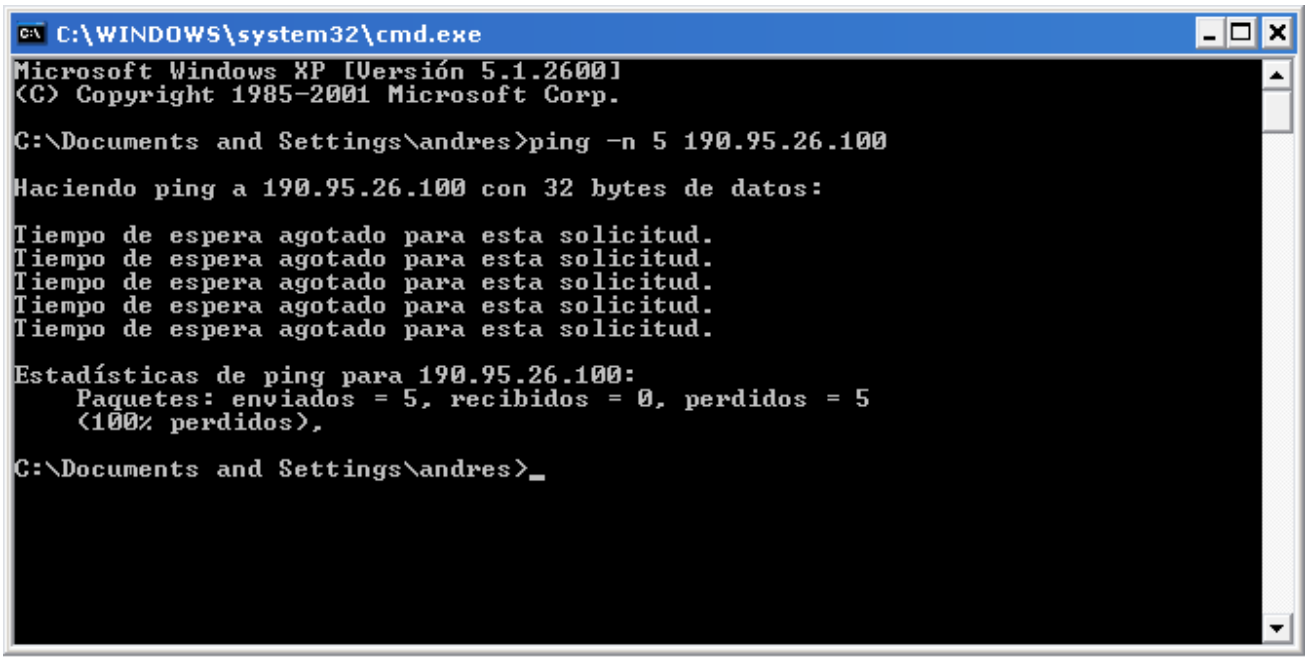


Figura N° 2.2 – Comando Ping sin asociación de Equipo

Como se puede ver que los datos enviados a esta dirección no obtuvieron respuesta (se perdieron) por lo tanto esta dirección no tiene ningún equipo asociado.

Ahora se prueba con la siguiente dirección 190.95.26.125 y en la figura N°2.3 se pudo apreciar lo siguiente:

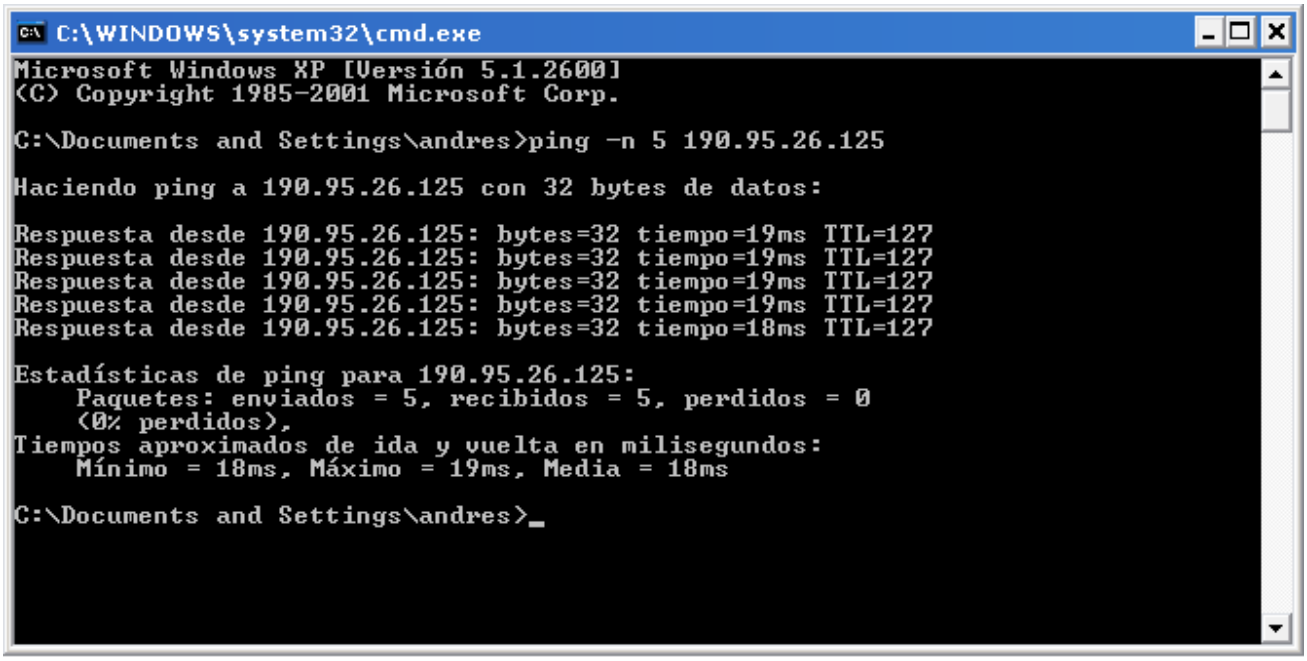


Figura N° 2.3 – Comando Ping con Asociación de Equipo

Bajo esta dirección se obtuvo 100% de respuesta de los datos enviados, por lo tanto la dirección IP existe en un equipo.

Mediante este comando entonces, se pudo apreciar la existencia de al menos un equipo en una Red.

Una vez descubierta la existencia de al menos uno de los equipos del dominio, un atacante podría obtener información relacionada con la topología o la distribución física y lógica de la red, mediante alguna aplicación de administración, como por ejemplo, Tracert.

El funcionamiento de Tracert se basa en la manipulación del campo TTL (determina el tiempo de los paquetes de datos) de la cabecera IP de un paquete, de forma que es capaz de determinar uno a uno los saltos por los que un determinado paquete avanza por la red TCP/IP. El campo TTL actúa como un contador de saltos, viéndose reducido en una unidad al ser reenviado por cada dispositivo de encaminamiento. Usando Tracert, con sus respectivas opciones se puede apreciar lo siguiente:

Se procede a escribir el comando Tracert en CMD con la opción -h (donde h es el número de saltos realizados), con la dirección 190.95.26.125.

Con ésta dirección se podrá volver a verificar la existencia de equipos, además de ver que empresa se asocia al servicio asignado [26]**.**

Con el siguiente ejemplo se prueba con un h=4, para realizar la verificación de validez, el Host asociado a la conexión y la interacción de ruteo de dirección con el servidor de surnet:

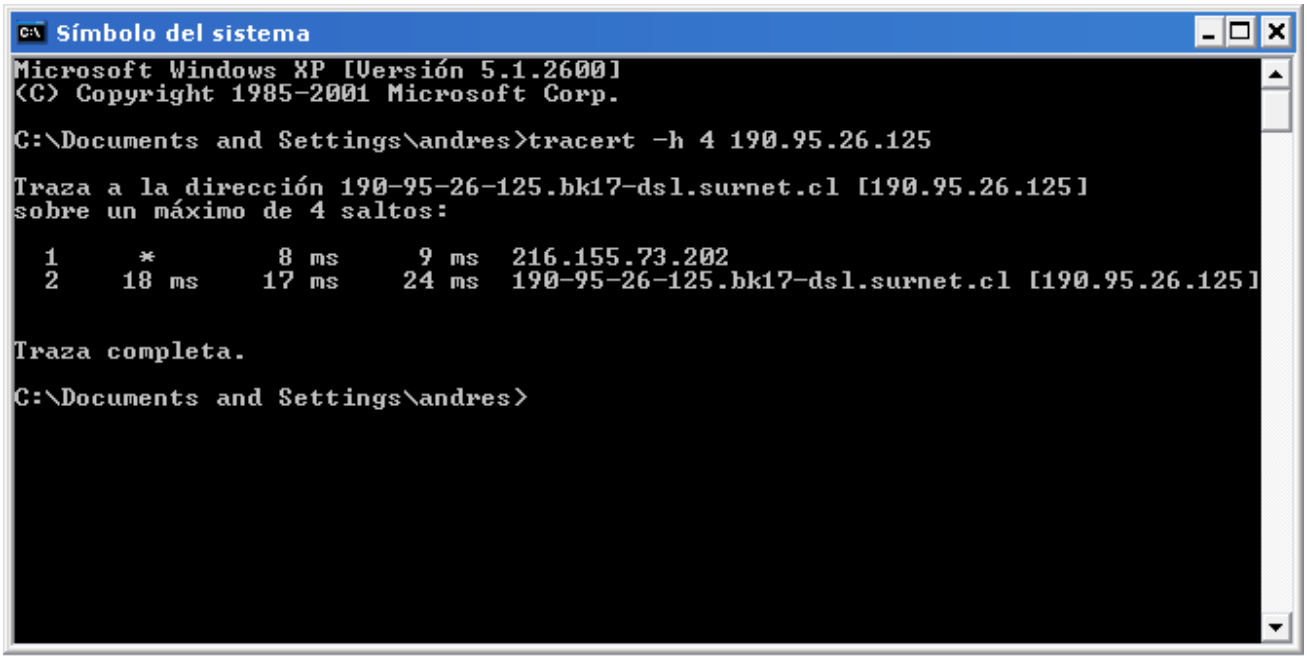


Figura N° 2.4 – Comando Tracert

2.1.1.1 *Formas de descubrir usuarios usando herramientas de administración*

Algo que puede determinar de manera clara el acceso a una red o equipo determinado, está directamente relacionado con identificar el número de usuarios y el nombre de ellos, por ello a continuación se nombraran las principales formas de acceder a esta información mediante las siguientes condiciones, usadas en conjunto con las nombradas anteriormente:

2.1.1.1.1 *Información de dominio*

Uno de los factores importantes que puede ser de gran ayuda a un atacante, es la asociación de dominios de un sitio u organización que pueda entregar información. De ésta forma, el atacante no tendrá acceso a la fuente principal, pero por medio de los dominios asociados a ellas tendrá acceso a sus Subredes. Dependiendo de la información que obtenga finalmente, puede tener acceso a la fuente principal. Una de las formas más accesibles, es usar consultas al servicio de dominios.

El tipo de consultas a éstos dominios, puede realizarse usando utilidades tales como Host, Dig, Nslookup y una de las más utilizadas Whois (más detalle en ítem 2.1.1.1.3).

Es así como el atacante puede obtener información relevante de la especialización de la red, es decir, cuales son sus alcances, su desarrollo, la red que soporta y los sistemas operativos con cuales trabajan los equipos que soportan la red. Éste punto es de vital importancia, ya que el atacante puede centrar su capacidad de ataque al saber qué sistema operativo usa la maquina.

2.1.1.1.2 *Cadenas de identificación*

Continuando con este proceso de recolección de información e identificación, asociando nuevos dominios y sistemas, se podrá tener un campo de ataque mucho mayor y el atacante podrá seguir identificando falencias que le puedan servir para adquirir mas experiencia en sistemas que posean una mayor seguridad. En éste proceso de incremento de información relevante, se encuentran las cadenas de identificación de texto, las cuales se pueden apreciar cuando un usuario se conecta a un servicio determinado usando alguna de las herramientas nombradas anteriormente (cuando accede a un servidor Web determinado, Ej. www.movistar.cl). En estas cadenas se puede ver el tipo de servicio asociado a una red, el tipo de

servicio que brinda cada servidor y la aplicación que está ejecutando para entregar ese servicio.

2.1.1.1.3 *Exploradores de Internet*

Para finalizar el análisis primario de búsqueda de información usando herramientas de administración, encontraremos una herramienta que es de fácil uso para cualquier persona con acceso a Internet y que tenga instalado un navegador o explorador en su computador. Mediante el uso de éste y solicitando conexión a un navegador, se puede establecer una petición de información. Esto es de tan fácil acceso, que el atacante puede hacer la consulta al buscador con solo el nombre de la organización de la cual desea información. El resultado de esta búsqueda puede entregar información general que el atacante puede utilizar para comenzar un sondeo de forma más sustancial. Mediante ésta forma, el atacante puede identificar personas (usuarios) que se vinculan a la organización, tecnología de los equipos con los que opera, entre otros aspectos.

Con Internet se tiene acceso a muchas herramientas y servidores especializados en buscar información, con los cuales se puede hacer un exhaustivo análisis. Un servidor especialista en ello es www.networksolutions.com el cual entrega variadas herramientas en la búsqueda de información, tales como Whois, que permite acceder a información relacionada con los Servidores de Nombre de Dominio (DNS), administración del servidor, dirección de correo asociada a la administración, entre otros datos.

A continuación se mostrará la secuencia realizada para poder identificar las variables asociadas a ésta herramienta y la información que entrega:

Como primer paso se accede al servidor por medio de la dirección anteriormente señalada, usando el explorador Explorer 8.0.

Figura N° 2.5 – Servidor de Nombres de Dominio

Luego se accede a For Web Professional, que es donde se encuentra la herramienta Whois que permitirá realizar la búsqueda de información.

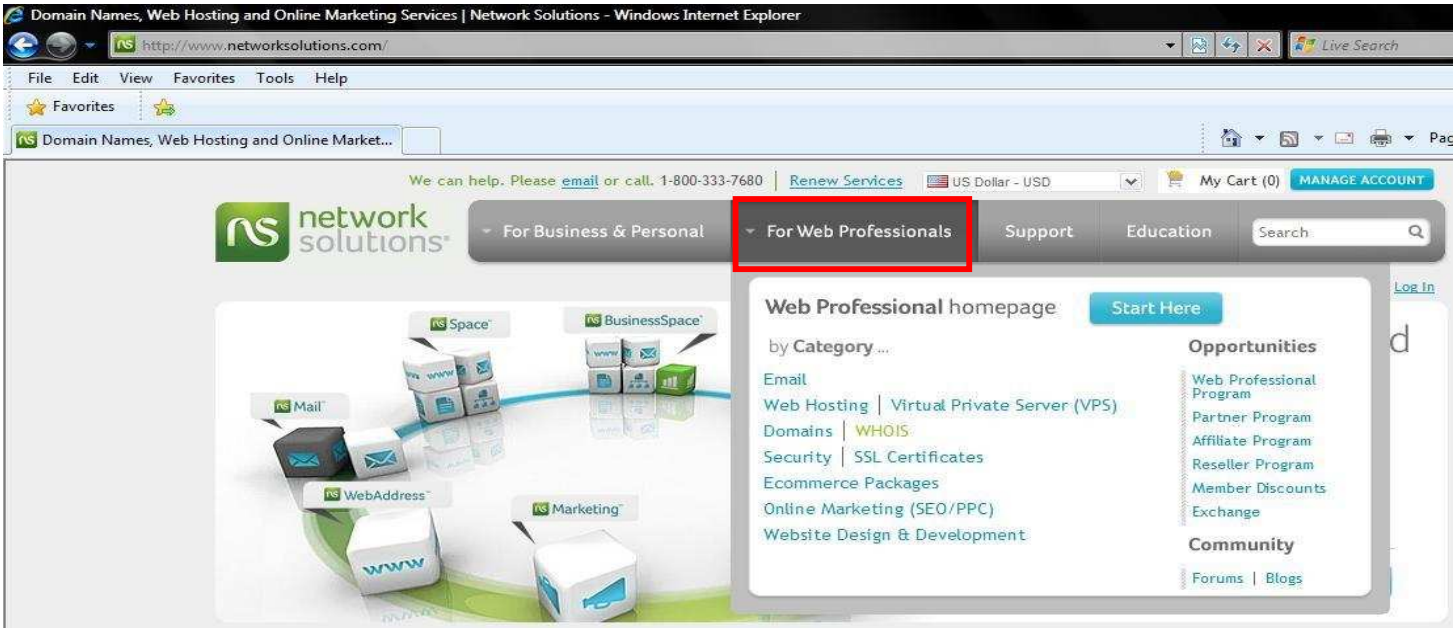


Figura N° 2.6 – Herramienta For Web Professionals del servidor

Posteriormente se ingresa a la herramienta Whois:

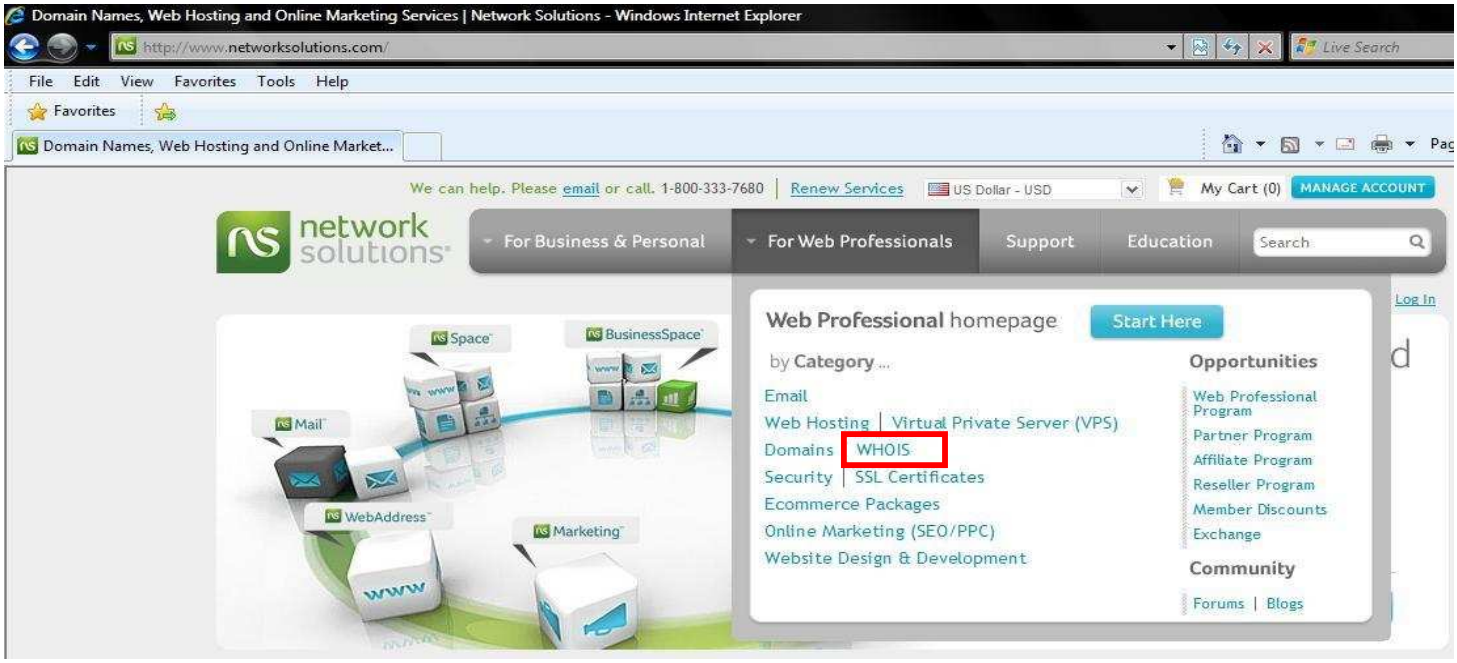


Figura N° 2.7 – Herramienta Whois del Servidor

Una vez de haber ingresado a Whois, se verá un buscador de dominio de nombres de servicio, donde podemos escribir el nombre del dominio u/o organización de la cual deseamos obtener información:

Figura N° 2.8 – Buscador de Dominios en Whois

A continuación se procede a escribir una dirección, para realizar la búsqueda de información, esta dirección será por ejemplo, microsoft.com:

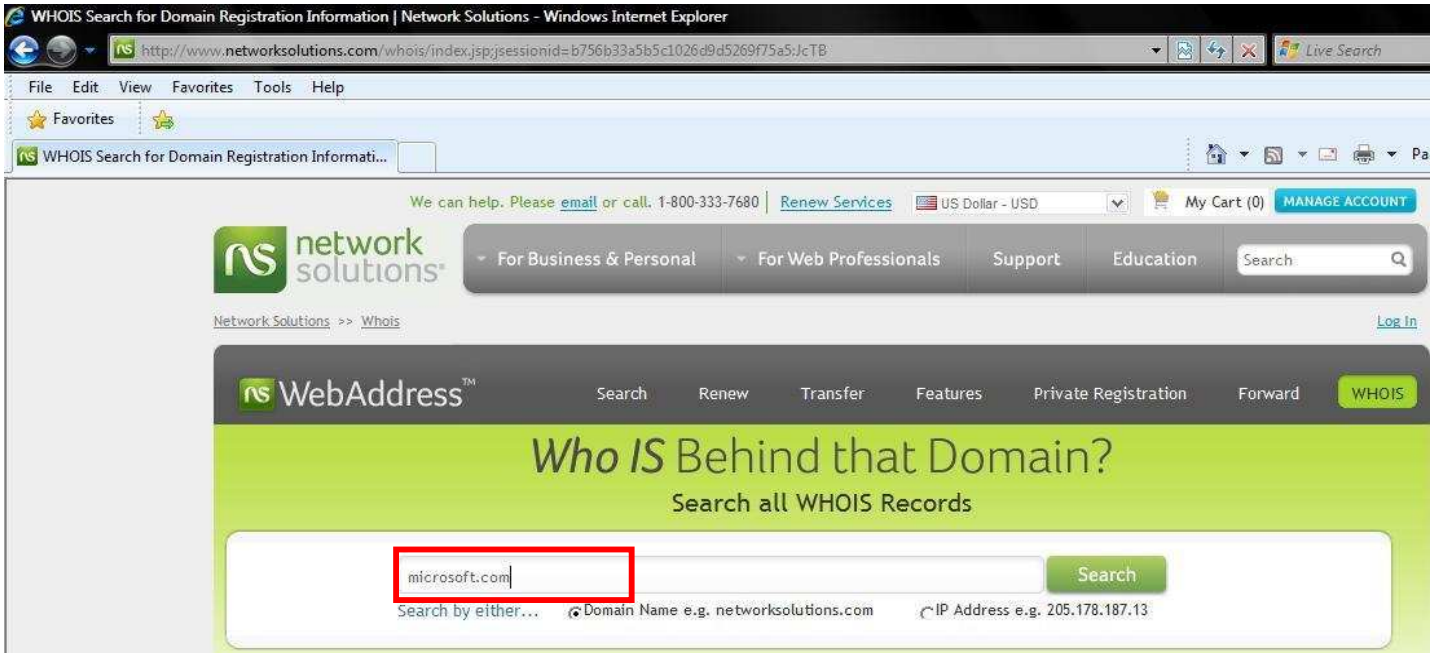


Figura N° 2.9 – Buscando Domínios de Microsoft.com

Una vez que se presiona la tecla buscar, se entregarán los datos asociados a esta dirección que ingresamos (Información que fue detallada anteriormente):

Figura N° 2.10 – Resultado de Búsqueda

De ésta forma se obtuvo información que junto a otra herramienta, puede permitir el acceso a la red que sustenta esta dirección y causarle más de algún inconveniente.

2.1.2 ***Especificación de aspectos más complejos en la búsqueda de información***

En relación al análisis realizado, se puede ir considerando un grado de inspección mucho mayor, por ello en este ítem se considerará un nuevo concepto en la recolección de información, el que se conoce como Fingerprinting, el cual es un proceso de búsqueda de huellas identificativas. Éste concepto es más profundo que los métodos nombrados anteriormente, el grado de precisión es considerado, ya que mediante su uso entregará datos más concretos, permitiendo realizar un análisis de los pasos o movimientos que hace un usuario o administrador de la red, es decir, se pueden apreciar los movimientos de información que fueron realizados anteriormente en la red o en el equipo que se desea buscar.

El proceso de búsqueda más especializado podrá favorecer la identificación de los siguientes aspectos:

2.1.2.1 *Mecanismo de control TCP asociados a la búsqueda*

En la búsqueda de nuevos elementos que se necesitan para realizar un ataque con características más especificas, encontramos la identificación de huellas, las cuales servirán para dar paso a la identificación de forma clara del sistema operativo con el cual opera el computador que se está analizando. Sumado a esto, se debe considerar la información obtenida con los métodos nombrados anteriormente, lo cual en conjunto, podrá ser un complemento importante para realizar una identificación más exhaustiva de los servicios que ofrece el sistema.

De éste modo, teniendo acceso a la identificación de paquetes de datos que son enviados a través del protocolo TCP, y que a su vez permite la correcta recepción de éstos paquetes, se puede realizar una interpretación de documentos técnicos y notas que circulan por la red. Éste proceso se conoce como Requests for Comments (RFC) y que mediante su análisis permite tener un porcentaje bastante elevado de las características más especificas del sistema operativo con el cual opera el computador vulnerado (las probabilidades de tener datos concretos son más altas), pudiendo ser versión del sistema operativo, complementos, añadidos entre otros aspectos [17]**.**

2.1.2.2 *Respuestas de Protocolo de control de mensajes de Internet. (ICMP)*

Para seguir realizando el análisis, se debe considerar de mucha importancia los alcances que puede tener el uso del protocolo ICMP en la búsqueda de información. En sí, el protocolo ICMP se encarga de realizar un control de flujo de datagramas IP que circulan por la Red, es decir, se encarga de realizar las notificaciones de posibles errores y de situaciones anormales que se presenten en el envío o recepción de información a través del protocolo IP, por lo tanto, un uso indebido de esto puede generarle a un atacante varias nuevas opciones de identificación de información [6]**.**

Al usar los comandos y ejecuciones (comando Ping) en cualquier sistema operativo, más esta nueva forma de saber sobre posibles problemas en el envío de información, se puede determinar que sistema está activo o sobre qué dirección IP está en funcionamiento.

La función que tiene el protocolo ICMP es de poder brindar una respuesta frente a algún tipo de conflicto presente con el envío o recepción de información, bajo ésta forma existen tres conceptos asociados al protocolo ICMP, la cuales son: ICMP Echo, ICMP Timestamp y ICMP Information.

ICMP Echo : Se puede establecer una petición de respuesta de recepción, es decir, si los datos en cuestión llegaron a destino de la misma forma que fueron enviados (similitud de datos enviados y recibidos) y poder determinar respecto a ello la comprobación de direcciones validas.

ICMP Timestamp : Se puede establecer una solicitud de confirmación de dónde provienen los datos enviados y en qué periodo fue realizada la solicitud.

ICMP Information : Se establece una confirmación de dirección IP o autoconfiguración, tanto de la dirección IP del equipo, como el de la dirección IP del servicio ofrecido en la red.

Estos tres conceptos deben tener siempre una respuesta de las solicitudes de información realizadas, es allí donde se pueden comenzar a considerar nuevas formas de vulnerar algún sistema en base a confirmaciones falsas o suplantaciones.

2.1.3 *Búsqueda de información en puertos TCP y UDP*

2.1.3.1 *TCP*

La búsqueda de información en puertos es un sistema que permite realizar la identificación de conexiones validas, tanto del origen como en el destino por medio de numeraciones lógicas que se asignan a cada tipo de conexión, pudiendo realizar uso o no uso de los servicios que puede ofrecer una conexión determinada. La condición de uso permite a un puerto tener tres estados los cuales son: abierto, cerrado y bloqueado [3]**.**

Por lo tanto, por medio de los puertos se puede determinar en una primera instancia el tipo de servicio que ofrece un equipo determinado o una

red. Entonces teniendo en conocimiento éstas condiciones, se puede comenzar a hacer un análisis en base a los posibles inconvenientes que existan o los inconvenientes que se presenten en algún puerto.

Para poder realizar una conexión a través de un puerto, se deben considerar que ésta se hace en base a 3 pasos, en los cuales se hace un intercambio de información para ver la validez de la solicitud [6]**. Éstos pasos son:**

Paso 1 : Se envía un paquete de datos de tipo SYN, donde el SYN es un Bit de control que permite realizar una petición de conexión.

Paso 2 : El paquete enviado en el paso 1 es recibido, y con una nueva instrucción llamada SYN/ACK se le da una respuesta a la petición del paso 1, por lo tanto SYN/ACK seria un Bit de respuesta a la solicitud de conexión.

Paso 3 : Finalmente, el paso 3 da el inicio a la sesión, con una instrucción llamada ACK, el cual es un Bit de confirmación del paso 2, es decir, si la respuesta a la petición fue aceptada por SYN/ACK, se podrá poner inicio a la sesión.

Considerando éstos pasos como la base para establecer una conexión [16]**, se puede comenzar a realizar una búsqueda de información en los puertos, por ello se nombrarán 2 formas con las cuales se puede obtener información:**

Escaneo de conexión TCP : Mediante ésta forma se realiza un análisis de los tres pasos anteriormente mencionados, y se considerará como información relevante aquellas conexiones que se encuentren iniciadas, luego de ello se podrá realizar una suposición en el puerto que dio inicio a la sesión, usando alguna herramienta.

Escaneo TCP SYN : Éste tipo de obtención de información ésta dado por solo enviar paquetes de datos SYN, revisando cada puerto y estableciendo peticiones para ver cual es disponible y cual no. Sirve para realizar una discriminación de los puertos activos. Para ello si, la petición de conexión existiera, una respuesta de tipo RST-ACK indicará que no hay ningún puerto disponible para iniciar sesión. Si llegara a existir un puerto disponible y listo para el inicio de sesión, la respuesta que se obtendría sería de tipo SYN-ACK (paso 2), por lo tanto, es un indicador de existencia. Luego de tener la respuesta, se debe realizar una negación por parte del atacante para no ser descubierto, la cual sería el envío de un paquete de datos RST-ACK, que en este caso, corta el inicio de sesión y el objetivo del atacante está cumplido, el cual era ver la disponibilidad de puerto, por lo tanto el atacante tendrá ese puerto en consideración, ya que está vulnerado para un posible análisis más complejo [1]**.**

Una ventaja que tiene el análisis de los puertos, es que no se puede identificar el punto de origen de la exploración.

Es importante establecer que los métodos nombrados anteriormente permiten al atacante conocer y establecer sus primeras percepciones de lo que desea atacar, utilizando para ello el uso de Softwares espías conocidos como Escuchas. Estos Softwares permiten realizar las peticiones nombradas en cada tipo de escaneo. El uso de estos Softwares puede ser utilizado en cualquier sistema operativo. Para Windows, existen gran variedad de Softwares, pero los más populares son el Winscan, Superscan e IPeye. Para Linux, uno de los más comunes y que mejor respuesta de ejecución tiene, es el Strobe.

Para apreciar un ejemplo de escaneo se visualizó el Software Superscan.

En la siguiente secuencia de imágenes se puede apreciar la configuración del Software. En el se debe establecer los puertos que se desean analizar, el periodo de realización, entre otras condiciones e información adicional que tiene que ver con la configuración del análisis:

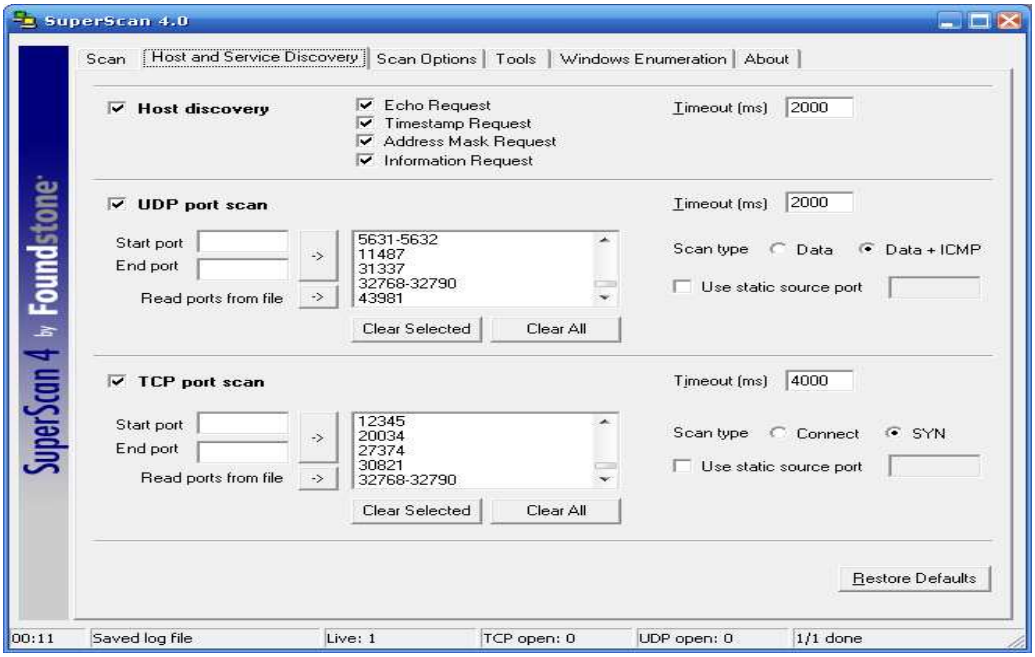


Figura N° 2.11 – Configuración Host and Discovery de Software SuperScan

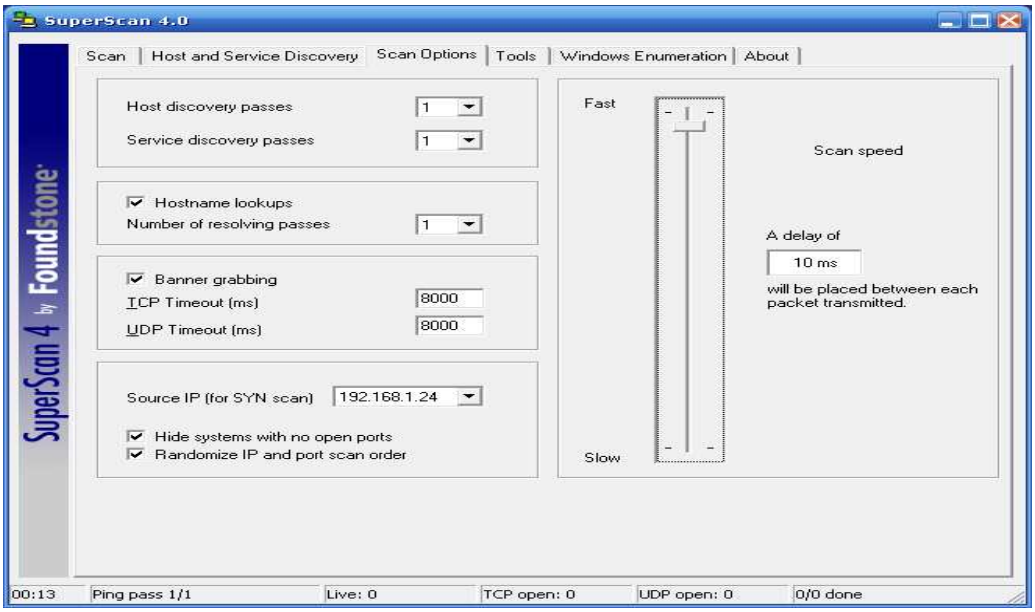


Figura N° 2.12 – Configuración Scan Option de Software SuperScan

Una vez realizada la configuración se procede a ejecutar la opción de búsqueda, donde es anotada la dirección IP analizada anteriormente y la máxima capacidad de operación de esa dirección asociada a una Red.

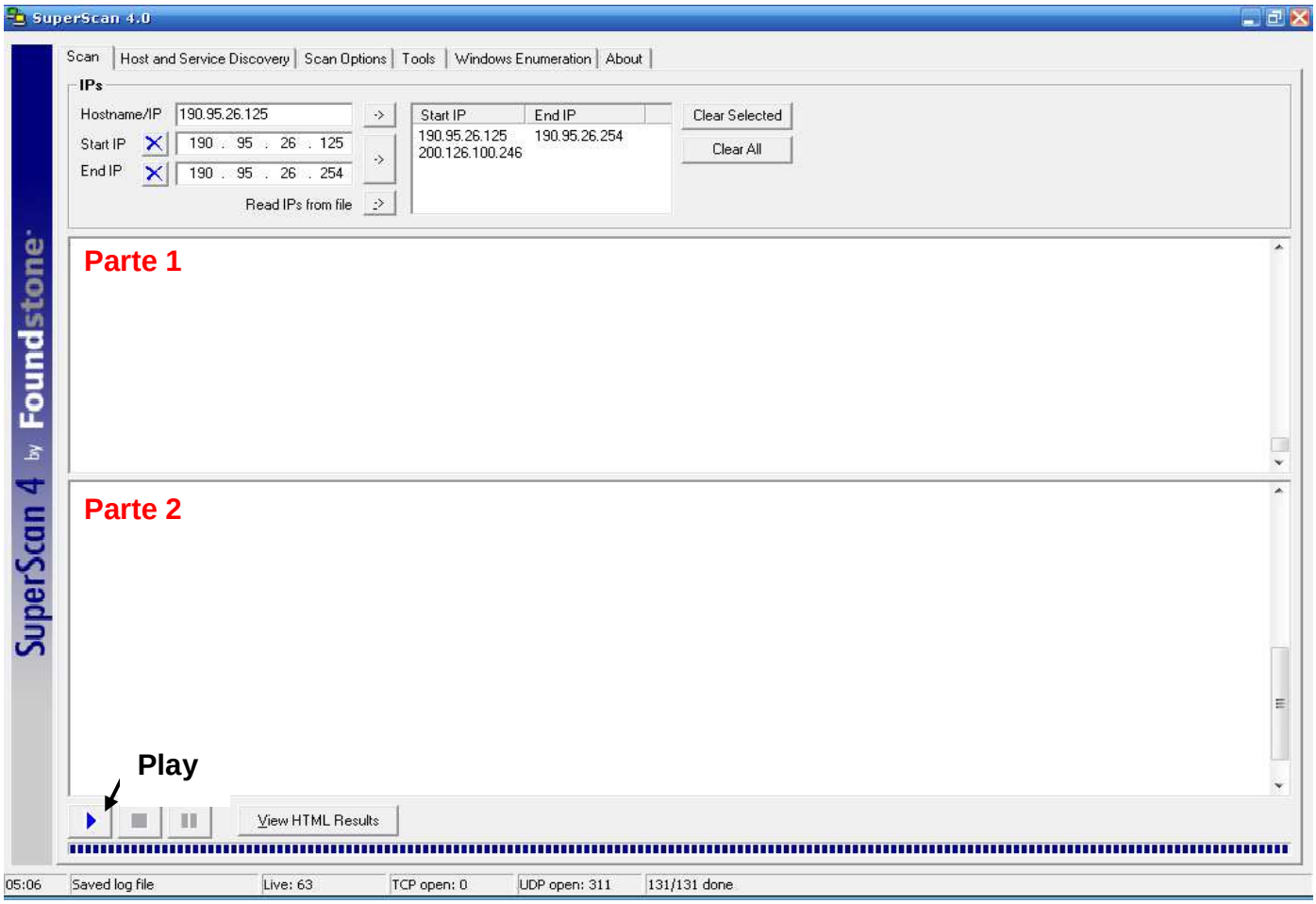


Figura N° 2.13 – Resultado de búsqueda SuperScan

Una vez que se ejecuta la opción presionando Play apreciamos 2 partes, en donde se encontrará información específica asociada a los puertos abiertos y otra parte un poco más general, como lo muestran las siguientes figuras:

Parte 1

```
Live hosts this batch: 63

190.95.26.126
   Hostname: 190-95-26-126.bkl7-dsl.surnet.cl
   UDP ports (4) 123,445,500,1900

190.95.26.127
   Hostname: 190-95-26-127.bkl7-dsl.surnet.cl
   UDP ports (3) 7,53,1900

190.95.26.129
   Hostname: 190-95-26-129.bkl7-dsl.surnet.cl
   UDP ports (4) 9,68,445,1900

190.95.26.130
   Hostname: 190-95-26-130.bkl7-dsl.surnet.cl
   UDP ports (6) 7,123,500,1900,1978,32773

190.95.26.137
   Hostname: 190-95-26-137.bkl7-dsl.surnet.cl
   UDP ports (84)
7,9,11,53,67,69,111,123,135,137,191,192,256,260,445,500,514,520,1009,1024,1025,1027,1028,1030,1033,1034,1035,1037,1041,1058,1091,1352
,1434,1645,1646,1812,1813,1900,1978,2002,2049,2140,2161,2301,2365,2493,2631,2967,3179,3327,3456,4045,4156,4296,4469,4802,5631,5632,11
487,31337,32768,32769,32770,32771,32772,32773,32774,32775,32776,32777,32778,32779,32780,32781,32782,32783,32784,32785,32786,32787,327
88,32789,32790,43981

190.95.26.138
   Hostname: 190-95-26-138.bkl7-dsl.surnet.cl
   UDP ports (1) 161

190.95.26.139
   Hostname: 190-95-26-139.bkl7-dsl.surnet.cl
   UDP ports (6) 9,123,445,500,1025,1900

190.95.26.153
   Hostname: 190-95-26-153.bkl7-dsl.surnet.cl
   UDP ports (1) 123

190.95.26.154
   Hostname: 190-95-26-154.bkl7-dsl.surnet.cl
   UDP ports (8) 9,123,445,500,1030,1034,1037,32788

190.95.26.156
   Hostname: 190-95-26-156.bkl7-dsl.surnet.cl
   UDP ports (5) 9,1025,1033,1037,1900

190.95.26.159
   Hostname: 190-95-26-159.bkl7-dsl.surnet.cl
   UDP ports (4) 9,123,500,1900

190.95.26.161
   Hostname: 190-95-26-161.bkl7-dsl.surnet.cl
   UDP ports (2) 137,138

190.95.26.162
   Hostname: 190-95-26-162.bkl7-dsl.surnet.cl
   UDP ports (7) 9,68,123,445,500,1033,1900

190.95.26.173
   Hostname: 190-95-26-173.bkl7-dsl.surnet.cl
   UDP ports (7) 123,500,1027,1033,1034,1900,32769
```

```
190.95.26.174
   Hostname: 190-95-26-174.bk17-dsl.surnet.cl
   UDP ports (4) 123,500,1033,1900

190.95.26.175
   Hostname: 190-95-26-175.bk17-dsl.surnet.cl
   UDP ports (5) 7,53,137,138,1900

190.95.26.182
   Hostname: 190-95-26-182.bk17-dsl.surnet.cl
   UDP ports (3) 123,500,1900

190.95.26.186
   Hostname: 190-95-26-186.bk17-dsl.surnet.cl
   UDP ports (4) 123,445,500,1900

190.95.26.188
   Hostname: 190-95-26-188.bk17-dsl.surnet.cl
   UDP ports (6) 9,123,1025,1034,1058,1900

190.95.26.192
   Hostname: 190-95-26-192.bk17-dsl.surnet.cl
   UDP ports (5) 9,123,445,500,1900

190.95.26.195
   Hostname: 190-95-26-195.bk17-dsl.surnet.cl
   UDP ports (5) 123,445,500,1034,1900

190.95.26.196
   Hostname: 190-95-26-196.bk17-dsl.surnet.cl
   UDP ports (5) 123,445,500,1900,2140

190.95.26.201
   Hostname: 190-95-26-201.bk17-dsl.surnet.cl
   UDP ports (4) 9,123,500,1900

190.95.26.206
   Hostname: 190-95-26-206.bk17-dsl.surnet.cl
   UDP ports (50)
9,11,53,67,68,69,111,123,135,137,191,445,500,520,1024,1027,1028,1033,1037,1058,1091,1645,1900,1978,2140,2161,2365,2493,2967,3179,3327
,3456,4045,4802,5632,32768,32769,32770,32771,32772,32773,32774,32775,32776,32777,32778,32781,32785,32789,43981

190.95.26.208
   Hostname: 190-95-26-208.bk17-dsl.surnet.cl
   UDP ports (6) 123,445,500,1028,1900,3456

190.95.26.209
   Hostname: 190-95-26-209.bk17-dsl.surnet.cl
   UDP ports (1) 32776

190.95.26.212
   Hostname: 190-95-26-212.bk17-dsl.surnet.cl
   UDP ports (1) 123

190.95.26.215
   Hostname: 190-95-26-215.bk17-dsl.surnet.cl
   UDP ports (5) 7,9,123,1030,1060

190.95.26.217
   Hostname: 190-95-26-217.bk17-dsl.surnet.cl
   UDP ports (2) 500,1900
```

```
190.95.26.218
   Hostname: 190-95-26-218.bkl7-dsl.surnet.cl
   UDP ports (4) 9,123,500,1900

190.95.26.221
   Hostname: 190-95-26-221.bkl7-dsl.surnet.cl
   UDP ports (4) 123,445,500,1900

190.95.26.228
   Hostname: 190-95-26-228.bkl7-dsl.surnet.cl
   UDP ports (5) 9,123,500,1027,1900

190.95.26.229
   Hostname: 190-95-26-229.bkl7-dsl.surnet.cl
   UDP ports (4) 123,445,500,1900

190.95.26.238
   Hostname: 190-95-26-238.bkl7-dsl.surnet.cl
   UDP ports (4) 123,500,1035,1058

190.95.26.244
   Hostname: 190-95-26-244.bkl7-dsl.surnet.cl
   UDP ports (3) 123,500,1900

190.95.26.251
   Hostname: 190-95-26-251.bkl7-dsl.surnet.cl
   UDP ports (39)
9,11,53,67,69,137,191,445,500,1027,1028,1033,1058,1091,1645,1900,1978,2140,2161,2365,2493,2967,3179,3327,3456,4045,4802,32768,32769,3
2770,32771,32773,32774,32775,32776,32778,32785,32789,43981
```

Figura N° 2.14 – Resultado de Búsqueda SuperScan

Esta primera parte entrega la siguiente descripción final:

```
Total live hosts discovered         63
Total open TCP ports                0
Total open UDP ports                311
```

Figura N° 2.15 – Resultado Global de Búsqueda con SuperScan

En la que encontramos un total de 63 Host disponibles y 311 puertos UDP Abiertos.

Segunda Parte

En la segunda parte ésta fue la información obtenida:

```
The IP list contains 131 entries
Service TCP ports: 179
Service UDP ports: 88
Packet delay: 10
Discovery passes: 1
ICMP pinging for host discovery: Yes
Host discovery ICMP timeout: 2000
TCP banner grabbing timeout: 8000
UDP banner grabbing timeout: 8000
Service scan passes: 1
Hostname resolving passes: 1
Full connect TCP scanning for service scanning: No
Service scanning TCP timeout: 4000
Service scanning UDP timeout: 2000
TCP source port: 0
UDP source port: 0
Enable hostname lookup: Yes
Enable banner grabbing: Yes

Scan started: 08/28/09 18:44:20

-------- Scan of 131 hosts started --------
Scanning 131 machines with 131 remaining.
-------- Host discovery pass 1 of 1 --------
Host discovery ICMP (Echo) scan (131 hosts)...
61 new machines discovered with ICMP (Echo)
Host discovery ICMP (Timestamp) scan (70 hosts)...
2 new machines discovered with ICMP (Timestamp)
Host discovery ICMP (AddrMask) scan (68 hosts)...
0 new machines discovered with ICMP (AddrMask)
Host discovery ICMP (Info) scan (68 hosts)...
0 new machines discovered with ICMP (Info)
TCP service scan (SYN) pass 1 of 1 (63 hosts x 179 ports)...
UDP service scan determining ICMP unreachable hosts pass 1 of 1 (63 hosts)...
UDP service scan pass 1 of 1 (63 hosts x 88 ports)...
Performing hostname resolution...
Performing banner grabs...
  TCP banner grabbing (0 ports)
  UDP banner grabbing (311 ports)
Reporting scan results...
-------- Scan done --------

Discovery scan finished: 08/28/09 18:49:27
```

Figura N° 2.16 – Descripción general de Búsqueda de SuperScan

Con ello entonces, es posible hacer un análisis de los puertos disponibles y así simular conexiones de acuerdo a lo señalado anteriormente.

2.1.3.2 *UDP*

El objetivo del análisis de los puertos UDP (protocolo de datagramas de usuario), es el mismo que el de los TCP, es decir, establecer bajo análisis la existencia de usuarios o conexiones disponibles [1].

Éste tipo de puerto, es una interfaz de las aplicaciones IP existentes, es una forma de multiplexar y demultiplexar los datagramas IP enviados a través de la red. Debido a estas multiplexiones y demultiplexiones se comienzan a generar datagramas UDP, que son un conjunto o subconjunto de datagramas IP.

En la figura N° 2.17 se puede apreciar la estructura de funcionamiento de los puertos UDP:

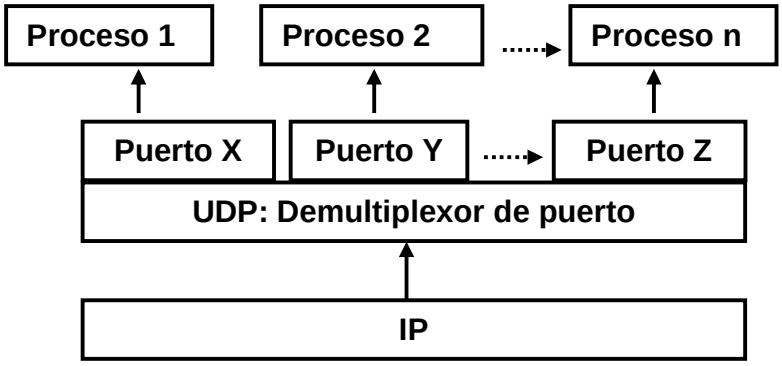


Figura N° 2.17 – Estructura de Puerto UDP

La forma para poder hacer búsquedas en estos puertos es simular el envío de datagramas, es decir, que se envíen datagramas UDP sin ninguna información. La ventaja de esto es, que si se genera una petición de sesión, y la sesión se encuentra disponible, el atacante entrará sin ninguna

respuesta a petición, solo entrará; por lo tanto, se crea una ventaja en el análisis, ya que no quedará registro de confirmación en el ingreso (no hay Paso 2). Si la sesión no llegara a estar disponible, se entrega una confirmación de puerto no encontrado del tipo ICMP.

Para el análisis tanto de los puertos TCP como los UDP, se usa una herramienta llamada Network Mapper (Nmap), la cual se encuentra disponible en la red. El real objetivo de esta herramienta, es realizar análisis de seguridad precisos en la red, tales como verificación de vulnerabilidades y confirmación de sistemas activos [6]**. Sin embargo, el mal uso de esta herramienta puede entregar datos importantes. Ésta herramienta se puede señalar que es un tipo de aplicación avanzada, que incluye muchos de los puntos tratados anteriormente sobre la inspección o análisis de los puertos e incluso del sistema operativo a una dirección asociada.**

A continuación se verá un ejemplo de cómo se realiza la exploración usando esta herramienta:

Primero, se establece la opción de scanme y se escribe la dirección IP que se desea analizar. En la figura N° 2.18 se pued e apreciar cómo se realizó la ejecución usando este Software [23]**:**

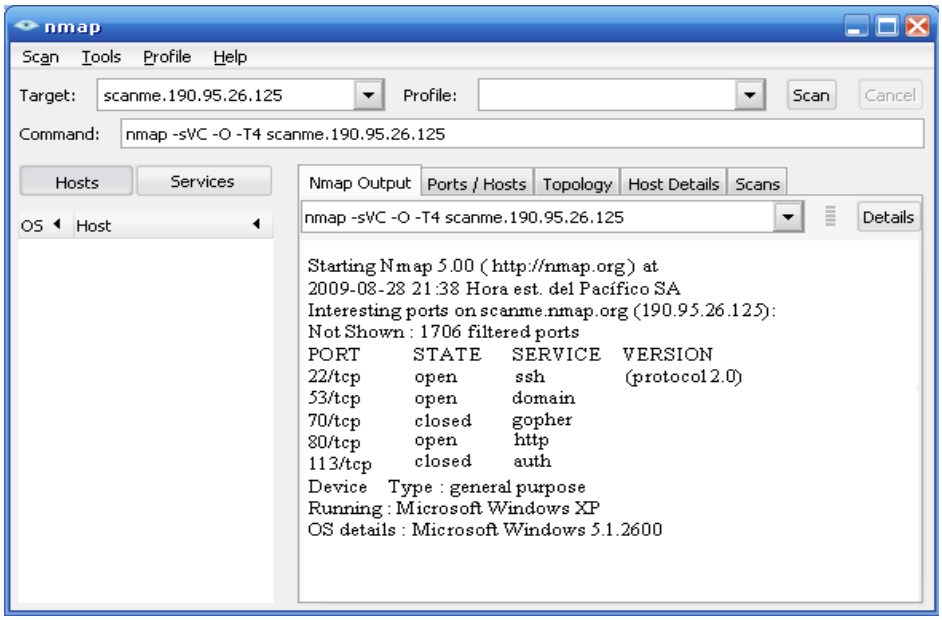


Figura N° 2.18 – Software Nmap

2.2 Interceptación de información en la Red

La interceptación de información en la red puede ser un factor que permite realizar la captura, análisis e interpretación de datagramas que circulan por una red. Éste proceso de interceptación es conocido como Sniffers [6]**. En sí, el Sniffers se conoce por ser un programa que opera en las 2 primeras capas del modelos TCP/IP y que su proceso de funcionamiento es en base a la información contenida en los paquetes TCP/IP. Ésta información puede ser captura y posteriormente analizada.**

El Sniffers como se señaló, es un programa y este programa trabaja en conjunto con la Tarjeta de Interfaz de Red (NIC), de ésta forma se puede absorber todo el tráfico que esté dentro de una red previamente establecida. Es allí su importancia, ya que con él se puede realizar una difusión masiva de interceptación a la dirección de la red y todas las direcciones IP bajo las que opera.

La forma cómo lo realiza, es tratando de adulterar la NIC, y establecer una condición de promiscuidad que permitirá recibir todos los paquetes que circulan por la red, por ello entonces, se debe colocar el Hardware de la red en modo promiscuo para que posteriormente se produzca el proceso de captura de la información. Lo que puede lograr con ello a su vez, es crear DNS para colocar un Software espía en éste dominio, estableciendo un tipo de respuesta inmediata frente a cualquier movimiento que se realice bajo el dominio.

2.2.1 *Vulnerabilidad de la MAC (Dirección de control de acceso al medio)*

Continuando con el método de interceptar información que circula por la red (Sniffer) se considerarán las vulnerabilidades en la MAC. La MAC es un número de la tarjeta de red, de 48 bits que identifica a cada máquina con

un número único. También se conoce como la dirección física de la máquina, después de haber establecido una conexión.

Las principales falencias están relacionadas con el acceso a la tarjeta de interfaz de red o al dispositivo Encaminador, su falencia en la configuración es un aspecto a considerar que permitirá activar o desactivar los filtros que posee la MAC. La desactivación de los filtros se conoce como modo promiscuo, el método nombrado anteriormente.

2.2.2 ***Vulnerabilidad de la ARP (Protocolo de resolución de direcciones)***

El protocolo ARP es el protocolo de la capa de Internet que se encarga de traducir las direcciones IP del Hardware con respecto a la dirección asignada por la MAC [6]**. De ésta forma se establece una relación, que permite a éste protocolo establecer una necesidad de cambio de la dirección IP hacia una dirección física (MAC). Esto da inicio a una petición de tipo ARP con una dirección establecida. A continuación se puede apreciar un ejemplo:**

Tenemos una dirección de difusión e identificación física; FF:FF:FF:FF:FF:FF, la cual es generada por un petición de tipo ARP que espera que un equipo que tenga ésta dirección conteste, con la dirección física de dicho equipo. En la figura N° 2.19 se est ablece la siguiente relación:

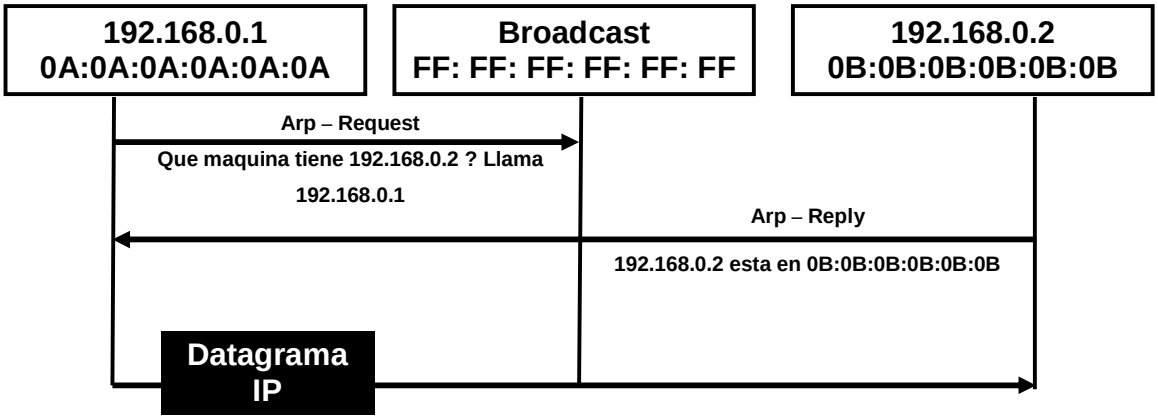


Figura N° 2.19 – Peticiones de Tipo ARP

En ésta figura se puede ver como una máquina con IP 192.168.0.1 y MAC 0A:0A:0A:0A:0A:0A solicita por difusión, qué dirección MAC está asociada a la IP 192.168.0.2. Por lo tanto, la máquina con IP 192.168.0.2 y MAC 0B:0B:0B:0B:0B:0B debería ser la única que respondiera a la petición.

Con el objetivo de reducir el tráfico en la red, cada respuesta de ARP (arp-reply) que llega a la tarjeta de red donde es almacenada en una tabla caché, aunque la máquina no haya realizado la correspondiente petición. De esta forma, toda respuesta de ARP que llega a la máquina es almacenada en la tabla de ARP de esta máquina. Éste factor se debe tener en consideración, ya que es la forma de poder tener acceso a una fuente de información para poder realizar suplantaciones de ARP y obtener las direcciones físicas de alguna maquina en particular a la cual se le desea sacar datos importantes [13]**.**

El objetivo de realizar una suplantación de ARP, es poder capturar tráfico de red, sin necesidad de poner en modo promiscuo la interfaz de red. Con éste método, se está manipulando la tabla de ARP de los equipos involucrados en la comunicación que se quiere capturar, se puede conseguir que el conmutador les haga llegar los paquetes. Si el engaño es posible, cuando las dos máquinas empiecen la comunicación, enviará sus paquetes hacia la máquina donde está el Software espía. Éste, para no descubrir el engaño, se encargará de encaminar el tráfico que ha interceptado.

En la figura N° 2.20 se puede ver como una tercera máquina se involucra en el reconocimiento de dirección de la figura anterior y da respuesta de tipo ARP para poder tener acceso a las tablas ARP y capturar el tráfico de red.

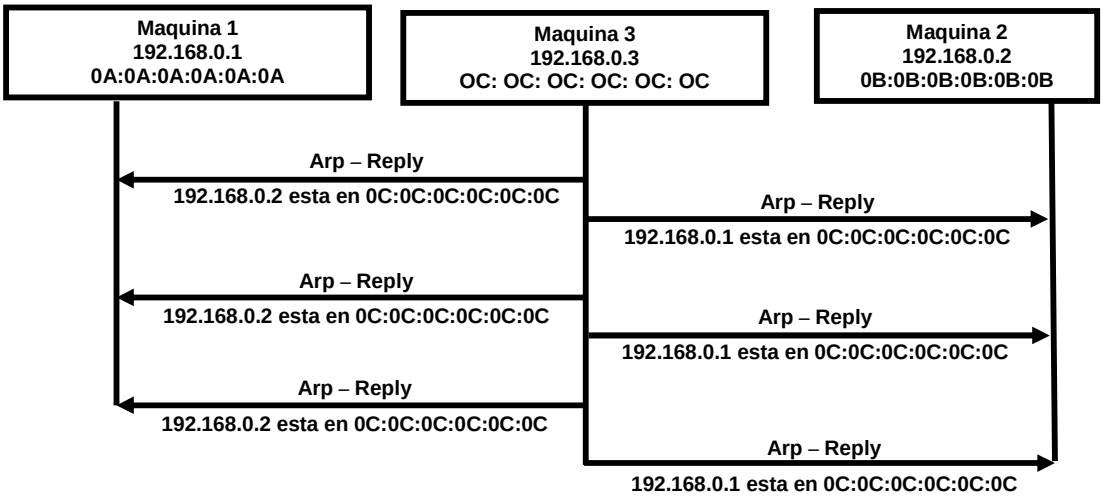


Figura N° 2.20 – Petición ARP con una tercera maquina intrusa

Con este método, toda comunicación entre las 2 máquinas pasaría por esta tercera máquina, ya que de ésta forma tanto la primera como la segunda, dirigen sus paquetes a la dirección MAC (0C:0C:0C:0C:0C:0C) de la tercera máquina establecida entre las 2.

El flujo de respuesta ARP (arp-reply) sería constante, para evitar que la tabla de ARP de las 2 máquinas se refresque con la información correcta.

Éste proceso corresponde a una suplantación ARP, y a partir del momento en que se haga efectivo el intercambio de información entre las dos máquinas, la tercera máquina podrá tener conocimiento de ello, y redireccionará la información hacia ella.

2.3 División de datagramas IP

Como se ha establecido, los datagramas IP son un parte del paquete que es enviado por la red y permiten realizar un mejor encaminamiento de los datos. El encargado de ello es el protocolo IP, que es el que selecciona un camino para estos paquetes.

Cuando se realiza un intercambio de información por las capas del modelos TCP/IP los datagramas IP son acondicionados para tener un tamaño determinado en las diferentes redes por la cuales pueden circular, por ello se establece un medida de los paquetes conocida como MTU (Maxim Transfers Unit) y ésta puede variar de acuerdo al medio físico empleado para la trasmisión de los datos.

Por lo tanto, de ésta forma el Protocolo IP establece que ningún paquete de datos enviados sea mayor que MTU.

Es por ésta condición que se realiza la división de los datagramas IP, para que éstos puedan ser trasmitidos por cualquier red, aumentando la rapidez en la llegada de los datos. Éste proceso de división también es conocido como Fragmentación [19]**.**

Sin embargo, a la hora del análisis, ésta condición es una vulnerabilidad presente ya que el protocolo IP no esta orientado a la conexión, no permite tener un control de flujo, recuperación de errores y una verificación o confirmación que los datos enviados han sido recepcionados.

Por ello, al realizarse muchas divisiones de los datos mientras viajan por diferentes redes, es posible que una persona pueda hacer mal uso de ello, realizando reensamblaje de los datos, búsqueda de huellas, exploración de puertos o cualquier otro método mencionado a la largo de este capitulo.

2.3.1 ***División de datagramas IP en la Red***

Para transmitir datagramas IP por la red, es necesario tener una unidad mínima de envío, la que se nombró y se conoce como MTU [1]**. Si la información que posee un datagrama IP llegara a hacer mayor que ésta unidad, éste datagrama IP deberá ser divido en varias unidades utilizando un Encaminador hasta lograr la unidad establecida y posteriormente reconstruirlos bajo algunas condiciones, que se nombrarán a continuación:**

Condición 1: Estas divisiones conocidas como fragmentos, deben estar asociadas a otro fragmento utilizando un identificador de fragmento común. Éste se clonará desde un campo de la cabecera IP, conocido como identificador IP (también llamado ID de fragmento).

Condición 2: Saber posición de la información en el paquete inicial (paquete no fragmentado). Parte del paquete al que pertenece para tener un ordenamiento eficaz de la información al momento de reconstruir el paquete.

Condición 3: Saber la longitud de la información de los datos transportados en el fragmento.

Condición 4: Cada fragmento tiene que saber si existen más fragmentos a continuación. Esto se indica en la cabecera, dejando o no activado el indicador de más fragmentos (Mas Fragmentos, MF) del datagrama IP.

Toda ésta información ira en la cabecera IP, colocada en el datagrama IP. Esto afectará a todo el tráfico TCP/IP puesto que IP es el protocolo responsable de la entrega de los paquetes.

En la figura N° 2.21 se mostrará un ejemplo de la configuración de un datagrama IP no fragmentado con un MTU de 1500 bytes:

Figura N° 2.21 – Configuración Datagrama IP no fragmentado con MTU de 1500 Bytes

Como se aprecia en la figura, en la primera parte se encuentra la cabecera IP, ésta es normalmente de 20 bytes, estará contenida la información necesaria para poder dirigir el datagrama IP hacia su destino (dirección IP de origen y destino, dirección del encaminamiento de origen, etc.).

Posterior a la cabecera IP, se encapsulan los datos. Éstos pueden ser tanto de un protocolo IP como TCP, UDP o ICMP. Por ejemplo, si estos datos fueran TCP, incluirían una cabecera TCP y datos TCP.

Teniendo en conocimiento como se comienza a realizar la división de la información en un datagrama IP con un MTU determinado, procederé a continuación a mostrar un ejemplo un poco más complejo en el cual se tiene un datagrama IP de 4068 Bytes y un MTU establecido por la red de 1500 Bytes. De éste modo, el datagrama de 4068 bytes deberá dividirse en 2 fragmentos de 1500 bytes y un fragmento un poco menor.

Estos paquetes fragmentados de 1500 bytes tendrán una cabecera IP de 20 bytes como fragmento inicial, quedando un máximo de 1480 bytes para los datos en cada fragmento.

En los siguientes pasos se examinara el contenido de cada uno de los tres fragmentos individuales que se formarán para que el datagrama de 4068 Bytes pueda ser enviado:

<u>Primer Fragmento</u> : La cabecera IP original se clonará para que contenga un identificador de fragmentos idéntico, tanto para el primer como para el resto de fragmentos. El primer fragmento es el único que contendrá la cabecera del mensaje ICMP (para evitar errores). Ésta no será clonada en los fragmentos posteriores. Como veremos más adelante, éste hecho identifica la naturaleza del fragmento original.

En la siguiente figura se puede apreciar el primer fragmento:

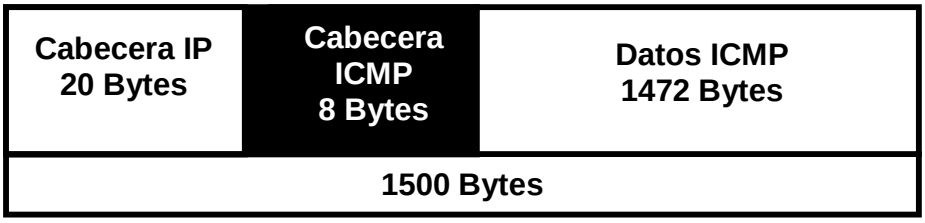
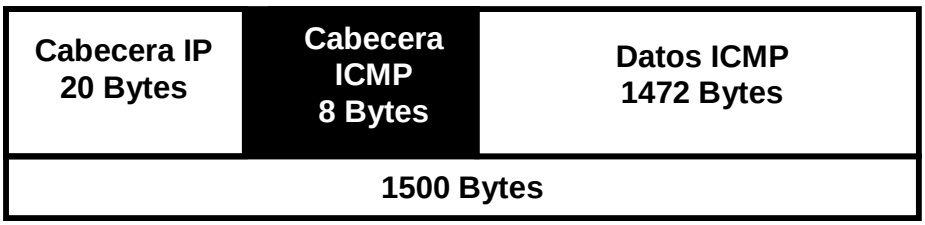


Figura N° 2.22 – Primer Fragmento

Además, éste primer fragmento tiene un valor de desplazamiento igual a 0, una longitud de 1480 bytes, 1472 bytes de datos, 8 bytes de cabecera ICMP y un indicador de más fragmentos. A continuación podemos observar con más detalle la configuración de éste primer fragmento:



Protocolo ICMP
ID de fragmento = 21223
Indicador de mas fragmentos = 1
Offset = 0
Longitud de los datos = 1480 Bytes

Figura N°2.23 – Detalle Primer Fragmento

Los primeros 20 bytes de los 1500 son la cabecera IP, y los 8 bytes siguientes son la cabecera ICMP. Recordemos que éste paquete fragmentado es una petición ICMP de tipo Echo (ver ítem 2.1.2.2) que tiene una cabecera de 8 bytes en su paquete original. Los 1472 bytes restantes son para los datos de ICMP. Además de los campos normales de la cabecera

IP, como origen, destino y protocolo (en éste caso ICMP) hay campos específicos para la fragmentación.

El identificador de fragmento, con un valor de 21223, es el enlace común para el resto de los fragmentos. El indicador de más fragmentos avisará de que el otro fragmento sigue al actual. Así pues, en éste primer fragmento, el indicador se establece en 1 para indicar que hay más fragmentos a continuación. Vemos también que se almacena el valor de los datos de éste fragmento en relación con los datos del datagrama completo. Para el primer registro, el valor de desplazamiento es 0. Finalmente, se almacena la longitud de los datos contenidos en este fragmento como la longitud del mismo, en éste caso, la longitud es 1480, es decir, la cabecera ICMP de 8 Bytes seguida por los primeros 1472 Bytes de los datos ICMP.

<u>Segundo Fragmento</u> : Se puede ver en la figura N°2.24 como en el segundo fragmento la cabecera IP de la cabecera original del primer fragmento es clonada con un identificador de fragmento idéntico:

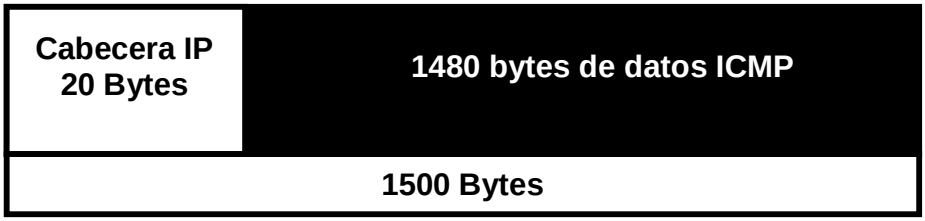
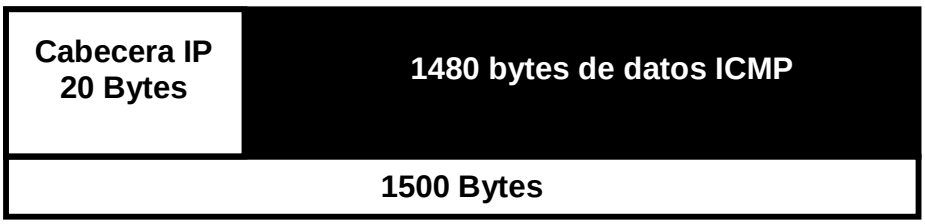


Figura N° 2.24 – Segundo Fragmento

Vemos también como se reproduce la mayor parte del resto de datos de la cabecera IP (como el origen y destino) en la nueva cabecera. Detrás de ésta van los 1480 Bytes de datos ICMP. Este segundo fragmento tiene un valor de 1480 y una longitud de 1480 Bytes. Además, como todavía le sigue un fragmento más, se activa nuevamente el indicador de más fragmentos.



Protocolo ICMP
ID de fragmento = 21223
Indicador de mas fragmentos = 1
Offset = 1480 Bytes
Longitud de los datos = 1480 Bytes

Figura N° 2.25 – Detalle Segundo Fragmento

La figura muestra el datagrama IP que lleva el segundo fragmento que, como el resto de fragmentos, necesita una cabecera IP de 20 bytes. De nuevo, el protocolo de la cabecera indica ICMP. El número de identificación de fragmento continúa siendo 21223. Y tiene el indicador de más fragmentos activado, porque hay otro fragmento a continuación.

Es importante tener presente que la cabecera ICMP del primer fragmento no ha sido clonada juntamente con los datos ICMP. Esto significa que, si se examinara tan solo este fragmento, no se podría saber el tipo de mensaje ICMP que hay almacenado. Este hecho puede suponer problemas importantes a la hora de utilizar dispositivos de filtrado.

<u>Tercer Fragmento</u> :

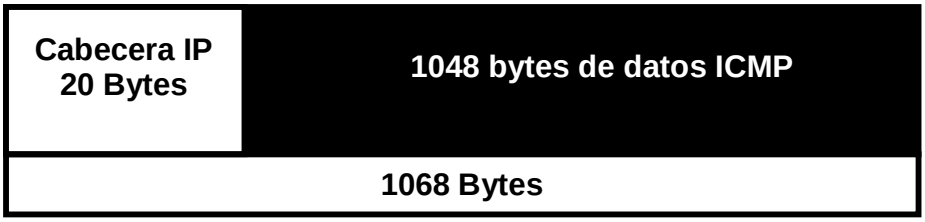
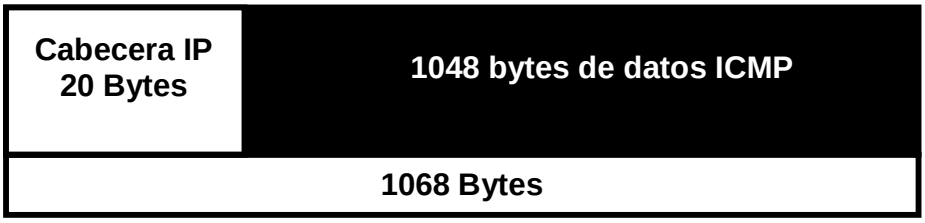


Figura N° 2.26 – Tercer Fragmento

En la figura N° 26 se puede ver cómo, una vez más ha sido clonada la cabecera IP de la cabecera original (con un identificador de fragmento idéntico). Los últimos 1048 Bytes de datos ICMP se insertan en éste nuevo datagrama IP. Éste fragmento tiene un desplazamiento de 2960 Bytes y una longitud de 1048 Bytes, y como no le siguen más fragmentos, el indicador de más fragmentos está desactivado. En la figura N° 2. 27 se puede observar con más detalle éste último fragmento:



Protocolo ICMP
ID de fragmento = 21223
Indicador de mas fragmentos = 0
Offset = 2960 Bytes
Longitud de los datos = 1048 Bytes

Figura N° 2.27 – Detalle Tercer Fragmento

Detrás de los 20 Bytes de la cabecera IP, encontramos en el fragmento el resto de bytes de los datos ICMP originales. El identificador de fragmento es 21223, y no se sigue estableciendo el indicador de más fragmentos porque éste es el último.

El valor de desplazamiento es 2960 (la suma de los dos fragmentos anteriores de 1480 bytes). Sólo hay 1048 Bytes de datos, es decir, el resto de Bytes del mensaje ICMP. Tanto éste fragmento como el segundo, no tienen cabecera ICMP, por lo tanto, el tipo de mensaje ICMP que nos indique que nos encontramos ante una petición Echo de ICMP.

En la figura N° 2.28 se puede apreciar el datagrama IP final bajo el análisis de los tres fragmentos detallados:

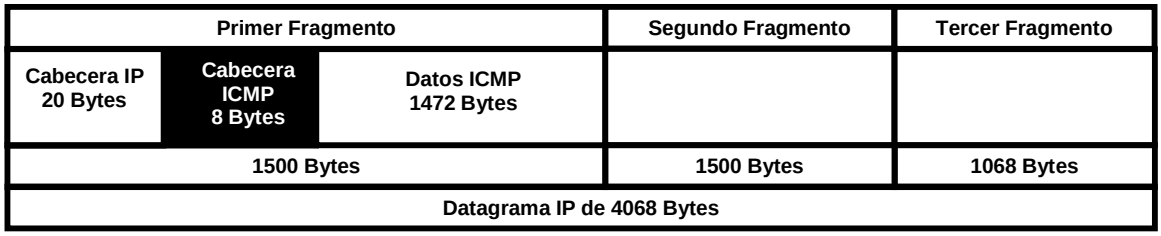


Figura N° 2.28 – Fragmento Completo

2.3.2 ***Fragmentación intencionada de datagramas IP***

Como se ha ido estableciendo, la fragmentación IP puede plantear una serie de problemas respecto a la seguridad de la red. Por ello, una de las problemáticas más destacadas, es la utilización de fragmentación IP malintencionada para burlar las técnicas básicas de inspección de datagramas IP que han sido mencionadas anteriormente.

Una de la formas, es que una persona pueda provocar intencionadamente una Fragmentación en los datagramas que envía a la red, con el objetivo de que pasen desapercibidos por diferentes dispositivos de prevención y de detección de ataques que no tienen implementado el proceso de Fragmentación y Reensamblado de datagramas IP [19]**.**

Es por ello que un factor importante, es la configuración de los dispositivos de prevención más básicos (Encaminadores con filtrado de paquetes, capitulo III), ya que las decisiones para bloquear paquetes se encuentran bajo esta opción y se basan generalmente en la información de cabecera de los paquetes (puertos TCP o UDP de destino). Esto significa que los paquetes TCP y UDP fragmentados, se pueden burlar más fácilmente aquellos mecanismos de prevención que no implementen el proceso de reensamblado para poder tener una visión global del paquete que hay que bloquear.

Una forma de dispositivos de prevención más avanzados (pasarelas a nivel de aplicación), así como en la mayor parte de los mecanismos de detección, las decisiones para detectar paquetes potencialmente peligrosos acostumbran a basarse nuevamente en la inspección de la cabecera del datagrama IP, así como en la parte de datos del paquete. Esto significa que la Fragmentación se puede utilizar nuevamente para burlar éste proceso de detección y conseguir que estos paquetes entren o salgan de la red de forma desapercibida.

Con el objetivo de descubrir la MTU de la red e intentar así realizar Fragmentación, el atacante puede utilizar el indicador de no Fragmentación del datagrama IP. Cuando el indicador de no Fragmentación está activado, como indica su nombre, no se realizaría ninguna Fragmentación en el datagrama. Por lo tanto, si un datagrama con éste indicador cruza una red en la que se exija la Fragmentación, el Encaminador lo descubrirá, descartará el datagrama y devolverá el mensaje de error al equipo emisor. Este mensaje de error ICMP contiene la MTU de la red que requiere la Fragmentación.

Es así como el atacante solo deberá construir datagramas con diferentes longitudes, con el indicador de Fragmentación establecido, a la espera de recibir estos mensajes de error.

Para solucionar el uso de la Fragmentación fraudulenta y garantizar una correcta inspección de paquetes, es necesaria la implementación del proceso de Fragmentación y el reensamblado de datagramas en dispositivos de prevención y detección. Esta solución puede suponer un coste adicional, ya que significa tener que examinar y almacenar cada fragmento. Aunque puede resultar muy costoso en cuanto a recursos (tiempo, proceso y memoria), será la única forma de asegurar que la inspección del paquete se ha realizado de forma correcta.

2.4 Denegación de servicio (DoS)

La denegación de servicio, es un término que se asocia a la forma de producir un bloqueo de un servicio determinado que utiliza un usuario válido, tanto en una red privada, como en la red global [10]. **Es así como se establece una forma de evitar que terceras personas puedan tener acceso a sitios o lugares que no están permitidos. Estos bloqueos pueden ser simplemente la limitación de acceso a una página Web.**

Las denegaciones, pueden ser realizadas por personas asignadas para tal hecho dentro de una red, por personas que no tienen en conocimiento el uso de una buena distribución del ancho de banda y así tener un mejor rendimiento, esto se ve reflejado cuando descargan archivos. Y también existe la posibilidad de que pueda ser hecha por personas ajenas a la red. Es de esta forma que se comienza a ver cómo afectarían las denegaciones de servicios a una red y sus equipos, provocando varios problemas en la ejecución y realización de un buen trabajo.

Por ello a continuación se mencionarán algunos inconvenientes bajo los que un atacante pueda beneficiarse:

2.4.1 Exceso de datagramas IP

Este tipo de ataques se realizan enviando una gran cantidad de datagramas IP por la red. Esto se realiza solo para producir un atochamiento de la información y lentitud en el tráfico de información, es así que se establece una forma de reducir el ancho de banda existente en la red. Este tipo de ataque es muy factible realizarlo en redes cuyo control de acceso no existe.

A continuación se hará mención a las formas en que se puede generar un mayor tráfico de información:

De tipo aleatoria : Este tipo de tráfico se produce cuando dentro de la red, la dirección de origen y de destino de un paquete determinado son falsas, estableciendo de esta forma una burla para identificar cual es el equipo de la red que está realizando el envío de información que comienza a colapsar el sistema.

De tipo definido : Es cuando dentro de la red, tanto la dirección de origen, como la de destino de un paquete, son identificadas en un mismo computador produciendo una gran cantidad de peticiones de servicio para este computador, de ésta forma el servidor comenzará a tratar de responder estas peticiones, produciendo una mayor lentitud y reduciendo el ancho de banda de toda la red.

Es así como se pasó a la utilización de varias formas de obtener información que se han mencionado en este capitulo, ahora necesarias para poder establecer una saturación o lentitud de la red. A continuación se procederá a identificar como generar solicitudes en los principales protocolos y puertos de comunicación, usando datagramas:

UDP : Generando un gran número de solicitudes UDP del tipo sin conexión, suplantación de conexión y verificación de puertos (ver ítem 2.1.3.2) se puede producir una lentitud generalizada de la red.

ICMP : Generando mensajes de control de flujo y error, bajo el envío de solicitudes de conexión y suplantación de acuerdo a las tres modalidades que tiene el protocolo ICMP que son la Echo, Timestamp e Information (ver ítem 2.1.2.2) se puede causar un atochamiento que permite reducir considerablemente el ancho de banda.

TCP : Al igual que el uso de los 2 puertos anteriores, con el TCP se desea lograr el mismo objetivo, es decir, producir la saturación de los

recursos que se están ofreciendo a la red bajo las vulnerabilidades del puerto TCP (ver ítem 2.1.3.1).

Cada vez que se procesa una conexión, deben crearse datagramas IP para almacenar la información necesaria para el funcionamiento del protocolo. Esto puede llegar a ocupar mucha memoria. Como la memoria del equipo es finita, es necesario imponer restricciones sobre el número de conexiones que un equipo podrá aceptar antes de quedarse sin recursos.

Esto puede hacer que el sistema que es víctima del ataque, sea incapaz de establecer cualquier conexión adicional para este servicio hasta que las conexiones que estén a la espera bajen el umbral. Hasta que se llegue a este límite, cada paquete SYN genera un SYN/ACK que permanecerá en la espera de establecerse para una futura conexión. Es decir, cada conexión tiene un temporizador (un límite para el tiempo que el sistema espera, el establecimiento de la conexión) que tiende a configurarse en un minuto. Cuando se excede el límite de tiempo, se libera la memoria que mantiene el estado de esta conexión y la cuenta de la espera de servicios disminuye en una unidad. Después de alcanzar el límite, puede mantenerse completa la espera de servicios, evitando que el sistema establezca nuevas conexiones en este puerto con nuevos paquetes SYN[1]**.**

Dado que el único propósito de la técnica es inundar la cola, no tiene ningún sentido utilizar la dirección IP real del atacante, ni tampoco devolver los SYN/ACK, puesto que de esta forma facilitaría que alguien pudiera llegar hasta el siguiendo la conexión. Por lo tanto, normalmente se falsea la dirección de origen del paquete, modificando para ello la cabecera IP de los paquetes que intervendrán en el ataque de una inundación SYN [6]**.**

La principal función del envío de excesivo de datagramas, es poder establecer la dirección de difusión de la red (dirección que causa que el sistema entregue una copia de un paquete a todas las computadoras de una red) como la dirección de destino de los datagramas IP, de esta forma los Encaminadores tendrán que enviar el paquete a todos los computadores de

la red, reduciendo el ancho de banda y produciendo deficiencias de los servicios.

2.4.2 Manipulación de la Fragmentación IP

Como he explicado en este capítulo, para que la información sea enviada y recibida de forma más expedita, es necesario realizar una Fragmentación en los datagramas, es en este proceso que también se pueden producir manipulaciones para beneficio de una persona que desee atacar una red y producir ataques de denegación de servicios [19]**. Es por ello que con la manipulación de este campo, pueden producirse problemas de compatibilidad en el sistema operativo de los computadores que se vean afectados dentro de la red, ya que el atacante manipulará o falseará la reconstrucción de los datagramas IP para producir el colapso del sistema operativo de la máquina afectada.**

A continuación en la siguiente tabla, se mostrará un ejemplo de cómo se realiza este falseo en la reconstrucción:

Se tiene un paquete de datos de 1024 Bytes con un MTU de 512 Bytes, por lo que será necesario realizar sólo 2 divisiones de 512 Bytes (2 fragmentos):

	Posición	Longitud
Fragmento 1	0	512 Bytes
Fragmento 2	512 Bytes	512 bytes

Tabla N° 2.1 – Detalle de Fragmentación Adecuada

Como lo muestra la tabla N° 2.1, los 2 fragmentos tendrán una longitud de 512 Bytes. Esta una distribución correcta de paquete que ha sido fragmentado.

Ahora en la tabla N° 2.2 se apreciará una manipulación en los datagramas fragmentados que permita realizar divisiones con longitud o MTU que no correspondan.

	Posición	Longitud
Fragmento 1	0	512 Bytes
Fragmento 2	500 Bytes	512 bytes
…….	…….	…….
Fragmento N	10	100

Tabla N° 2.2 – Detalle de manipulación de Fragmentación

Entonces el objetivo de modificar estos parámetros, es producir la falla en la reconstrucción o ensamblaje del datagramas que fue enviado. Esta falla es conocida como Buffer – Overrun.

2.4.3 Ataques de Denegación de Servicio tipo Ping

Este tipo de ataques, plantea que al igual que el método anterior, la manera en que se pueden manipular los fragmentos de los datagramas IP. El proceso se logra al obtener como referencia la máxima longitud que puede tener un datagrama IP, esta longitud es de 65535 Bytes, la que incluye la cabecera IP (20 Bytes) y la cabecera ICMP (8 Bytes), por lo tanto, la cantidad Bytes disponibles para datos del tipo ICMP seria de 65507 Bytes [20]**.**

Con estos datos y el uso del comando Ping, se establecen las nuevas condiciones y modificaciones para que el paquete de 65535 Bytes pueda tener un tamaño mayor por medio de la Fragmentación. De esta forma en el proceso de Fragmentación, se producirán desigualdades que llevarán a un atochamiento y lentitud de la red.

Principalmente lo que se realiza, es tener un solo fragmento de un tamaño muy cercano al mayor valor de datagrama, por ejemplo 65515 Bytes, con este valor de fragmento sólo para información, más los 20 Bytes de la cabecera IP y los 8 Bytes de la cabecera ICMP, se tendrá un valor de datagrama de 65543 Bytes, sobrepasando en 8 Bytes el tamaño máximo establecido. Este hecho provocara que al reconstruir el paquete original en el destino, se produzcan errores que, si existen deficiencias en la implementación de la pila TCP/IP del sistema, podrán causar la degradación total del sistema atacado.

2.4.4 Ataques de Denegación de Servicios tipo Email

En este tipo de ataque, se procede a enviar muchos mensajes idénticos a una o varias direcciones de Host. El efecto en el objetivo, es un alto uso del ancho de banda y menos espacio de disco. Cuando envías muchos mensajes a una dirección inexistente del Host desde otra inexistente, el mensaje crecerá debido a las cabeceras. Irá de un lado a otro creciendo. Por más odioso que se vea este ataque, es bastante efectivo.

Ejemplo: Envía un mail de 100KBytes a noexiste@host.atacado.com desde una dirección que no exista como noexiste@esta.direccion.zus Cuando el mensaje llegue a host.atacado.com , como no existe la dirección, no regresará el mensaje a noexiste@esta.direccion.zus y como ésta dirección tampoco existe, regresará ahora como un mensaje de 300k y así sucesivamente si se decide hacer con más cuentas de Email.

2.4.5 Ataques de Denegación de Servicios tipo DNS

El ataque DNS saca partido de las diferencias de tamaño entre una solicitud DNS y su respuesta, haciendo que todo el ancho de banda de la red esté atascado por falsas respuestas DNS[4].**El atacante, utiliza los servidores DNS como amplificadores, para multiplicar el tráfico DNS. El atacante**

comienza enviando pequeñas solicitudes DNS, que contienen la dirección IP manipulada de la victima, a cada servidor DNS. Las respuestas devueltas a las pequeñas peticiones son mucho mayores que si se devolvieran muchas respuestas al mismo tiempo, congestionándose el vínculo y produciéndose la negación de servicio. Una de las soluciones para este problema, es que los administradores configuren los servidores DNS para responder con una respuesta de rechazo, que tiene un tamaño mucho menor que una respuesta de resolución de nombre, cuando reciben las solicitudes DNS de fuentes sospechosas o inesperadas.

2.4.6 Ataques de Denegación de Servicios distribuidos

Este tipo de ataques se establece cuando varios equipos cooperan entre ellos para atacar a un equipo determinado, causándole una denegación de servicio [10]**. El flujo de mensajes de entrada que padece el equipo atacado, le dejará sin recursos y será incapaz de ofrecer sus servicios a usuarios legítimos.**

Ahora se señalarán los 2 principales tipos de ataques distribuidos:

Trinoo : El objetivo de Trinoo es poder acceder a un equipo determinado en conjunto con otros equipos, permitiendo detectar las vulnerabilidades de los servicios en los sistemas y crear listas de vulnerabilidades. Posteriormente a ello, se introducirán Softwares espías (ya mencionados) que permitan tener en conocimiento a los atacantes y crear una red espía, que irá creciendo e identificando vulnerabilidades en la red asociada a la máquina afectada [10]**.**

La relación que se da en este proceso, es una relación atacante - maestro - peones - usuarios, donde el atacante es el que controla a varios maestros, el maestro a varios peones y los peones son los que reciben la orden y producen finalmente el ataque a los usuarios. Estos ataques estarán basados en las vulnerabilidades de los puertos TCP y UDP (mencionada en

el ítem 2.3.2), de una forma más generalizada. Mediante estos inconvenientes, la consola de administración de la máquina afectada queda abierta para el acceso de los peones y lo que producirá finalmente el atochamiento y colapso del ancho de banda y de los servicios que esa máquina desee obtener.

Tribe Flood Network : El Tribe Flood Network procede de la misma forma que Trinoo, pero con ciertas mejoras en la ejecución, ya que sumado a la detección masiva de vulnerabilidades en los puertos TCP y UDP, se suman las vulnerabilidades existentes con el ICMP (ver ítem 2.1.2.2). De esta forma, los peones ejecutan las órdenes dadas, estableciendo peticiones de conexión de tipo ICMP y TCP produciendo un gran número de solicitudes de conexión de servicios que estancarán el sistema, y los servicios no podrán ser brindados. También pueden generarse modificaciones en la Fragmentación (longitud de datos y cabecera) y posterior colapso de los datagramas IP, ya que no habrá concordancia entro los datos enviados y los datos recibidos [6]**.**

Esta forma está dando pie a un nuevo sistema de ataque de carácter masivo, basado en las principales vulnerabilidades analizadas en los puntos anteriores. Las consecuencias por estos tipos de ataques, pueden producir serios inconvenientes con respecto a un servicio que se brinda. Un ejemplo de este ataque fue el ocurrido en el 2002 a amazom.com, la cual es una de las empresas Norteamericanas más grandes del mundo, la cual ofrece servicios de venta online en todo el mundo. El ataque masivo se centró en las peticiones de conexión (de tipo TCP y ICMP) y generación de conexión por parte de usuarios válidos, como no válidos. Esto fue ejecutado por una enorme cantidad de peones que en menos de 2 horas colapsaron el sitio, este colapso se mantuvo durante 2 días, este ataque produjo pérdidas cuantiosas a amazom.com. Posterior a ello, se comenzaron a generar mayores resguardos en estos tipos de servicios de compra online, que a la fecha tienen una seguridad de gran consideración.

2.5 Vulnerabilidades de programación en modelo TCP/IP

En este ítem se quiere mostrar cuales son los conflictos que presenta la programación asociada al funcionamiento, servicios y seguridad a nivel de sistemas de una red TCP/IP. Los problemas que se llegarán a presentar a nivel de sistemas, pueden llevar a un equipo o red a una ruptura general de servicios.

Las vulnerabilidades de programación, tienen como objetivo ingresar un código arbitrario en el sistema operativo sobre el que se está ejecutando la aplicación. Éste código arbitrario consistirá en la ejecución de un código en Assembler o C, el cual permite la posterior ejecución de comandos de sistema o modificaciones de las bibliotecas de vínculos dinámicos (DLL), como si fuera el administrador, es decir, con el acceso a todos los permisos.

Este código es conocido como Shellcode, el cual está asociado a un conjunto de órdenes con un objetivo específico. Se usa principalmente para explotar los errores del sistema causado por defectos de programación (Buffer Overflow), de tal forma que el programa afectado pretende escribir más información en la unidad de memoria (buffer) de la que puede guardar.

Los ataques que permiten explotar este tipo de vulnerabilidades, se presentan generalmente en forma binaria (programas ejecutables) ya compilados para el sistema operativo en el que se está ejecutando la aplicación vulnerable (Exploits) [28]**. Esta aplicación fuerza las condiciones necesarias para aprovecharse de un error de seguridad subyacente y así impedir el normal funcionamiento de la aplicación que se está ejecutando.**

Existen infinidad de aplicaciones vulnerables o Exploits para servidores y generalmente se pueden encontrar disponibles en Internet ya compilados o en forma de código fuente.

En La página http://mx.geocities.com/hackerss_one/exploits.htm se pueden encontrar una serie de Exploits, entre los más utilizados se encuentra el MESSENGER Microsoft Windows Messenger Service DoS 1 KB,

el cual es compilado en el equipo una vez que está instalado el Software original de MESSENGER.

A continuación se mencionarán 2 vulnerabilidades asociadas a la programación a nivel de aplicación:

2.5.1 Exceso de datos en Unidades de Memoria

El exceso de datos en una unidad de memoria, permite escribir información más allá de los límites que un registro de datos almacena, en la en la Pila (Lista estructurada de datos que almacena y recupera datos) de ejecución. A partir de este registro de datos, asociada a una llamada a función dentro del programa, se puede conseguir corromper el flujo de la ejecución modificando el valor de regreso de la llamada a la función. Si este cambio en el flujo de ejecución es posible, se podrá llevar la ejecución a una dirección de memoria arbitraria (introducida en los datos de la pila a partir del mismo ataque) y ejecutar un código malicioso.

Para poder generar un exceso de datos en la memoria, es necesario conocer la arquitectura del sistema en el que se está ejecutando el programa, así como su sistema operativo. A partir de esta información, será posible conocer, por ejemplo, el sentido de crecimiento de la pila de ejecución (puede ser a direcciones menores de memoria o a direcciones mayores) y la definición del puntero de pila (si este hace referencia a la última posición ocupada en la pila o a la primera posición libre).

Asimismo, se requiere conocer también en detalle el orden en el que se depositan los distintos elementos en la pila, la dirección de retorno (RET), el orden de las variables locales y ciertos parámetros extras asociados a la pila.

Con toda esta información, se podrá introducir un valor en la posición de la dirección de regreso que modifique el flujo de ejecución justo en el punto que se desee, es decir, una posición de memoria en el que se haya almacenado previamente el código que hay que ejecutar. Generalmente, éste

suele ser el código en ensamblador necesario para abrir una consola de sistema (Shellcode).

Como esta entendido, un programa tiene un área de código ejecutable, y usa en memoria un espacio para almacenamiento del propio código y también para almacenamiento de los datos que vaya a utilizar. De la misma forma, si el programa recibe parámetros o datos, debe guardarlos temporalmente en su memoria.

A continuación se hará mención a un ejemplo relacionado con el exceso de datos en la memoria:

Se tiene un programa servidor de páginas Web. Cuando el usuario teclea en un navegador la siguiente dirección http://www.microsoft.com/directx, el texto tecleado www.microsoft.com/directx viaja como dato al servidor Web de Microsoft. Dicho servidor es un programa que recibe ese texto, y que tiene que almacenarlo en memoria.

De esta forma se puede comenzar a suponer que, al ingresar datos desde un navegador, el texto sea del tamaño que se desee, es decir, sin tener un tamaño máximo para escribir. Es así como, se teclea la siguiente dirección http://www.microsoft.com/$xxxx_n$ y el texto que se digita en las $xxxx_n$ es de una gran envergadura.

De esta forma se supondrá el envío de 10.000 caracteres, para ver los efectos que puede provocar.

Si el programa servidor que se está ejecutando en los servidores de Microsoft no tiene presente que pueda recibir toda esta cantidad de datos, y el programador que lo ha realizado ha previsto sólo una cantidad, digamos razonable de 1.000 caracteres, el propio programa al intentar guardarse esos 10.000 caracteres, está desintegrando áreas de memoria que pueden ser de contenido de otros datos o incluso el código ejecutable del propio servidor. En cualquier caso, hay destrucción de información que provocará en el mejor de los casos, una caída del programa del servidor Web por desintegrar el mismo código de ejecución.

Este es un ejemplo muy sencillo, pero de él se pueden secar varias conclusiones respecto a lo que sucede.

Un programa, se descompone en varias funciones. Dicho programa recibe datos, se los guarda, y los pasa al resto de funciones o subprogramas que lo necesiten.

El problema es cuando el propio programa, los subprogramas o funciones, tienen reservados tamaños inferiores a la longitud de los datos que reciben.

Normalmente, los controles anteriores no se hacen, excepto en entrada de datos, debido a que esto implica sobrecargar excesivamente de código de comprobación, y en tiempo de ejecución todos los parámetros y todas las zonas de memoria a las que accede el programa.

El problema surge cuando muchas de las funciones diseñadas para ejecutarse internamente, y que no tienen controles de los parámetros, deciden reutilizarse en otros programas de nivel superior los cuales pueden no tener tampoco dichos controles. En este caso, y aunque su funcionamiento sea normal, pueden encontrarse situaciones en que alguien malintencionado comience a descubrir errores y decida vulnerar el sistema. Es vulnerable un programa de este tipo, desde el momento en que es posible desbloquearlo, si ello sucede, se podrá realizar lo que se desee con respecto a la manipulación del programa, es decir, tomar control de él.

2.5.2 *Copia de Cadenas de Caracteres*

El copiar caracteres en los datos de memoria, es otra vulnerabilidad asociada a la programación. Mediante ella se realiza una copia de las cadenas de formato de los datos de memoria, sin las comprobaciones necesarias, es decir, cuando el programa que soporta el sistema se encuentra habilitado o fue desbloqueado [29]**. El error de las cadenas de formato de la memoria, se produce cuando un programador quiere mostrar una cadena mediante unas de las funciones que admiten opciones de formato, tal como:**

Printf : Es un carácter usado en lenguaje C, que permite realizar funciones para imprimir números enteros, cadenas de caracteres y delimitar la longitud de los campos a imprimir. A su vez puede realizar descripciones de salida de información en la memoria de un programa e identificación de cadenas de formato.

Por medio de complementos o datos adicionales no especificados de este carácter en la instrucciones de ejecución (tales como Printf (%n), opción que maneja la cantidad de Bit de salida) se puede generar un agujero de seguridad en el código que permitirá controlar el flujo de la ejecución. A causa de este error, un atacante podría acceder a valores de la pila de ejecución que se encuentren por encima de una cadena de formato. Esta deficiencia le permitirá tener el control necesario para escribir en la memoria del proceso y alterar el flujo de la ejecución para llevarlo a una ejecución de código arbitrario (Shellcode).

CAPITULO III:

Primeras condiciones

de seguridad

asociadas a una

Red TCP/IP

1 *PRINCIPALES MÉTODOS PARA PREVENIR LAS VULNERABILIDADES DE UNA RED TCP/IP*

En este capítulo, los puntos a tratar considerarán la forma de prevenir la red de posibles ataques. De ésta forma se comenzará a dar un grado de confianza respecto a la seguridad que debe poseer cada red. La idea de ello, es que los equipos conectados a la red pueden tener un resguardo frente a algún inconveniente que se presente, ya sea éste ocasionado tanto por fallas internas, como por terceros que tengan intensiones de saboteo.

Por ello para comenzar el desarrollo respecto a este primer nivel en la seguridad de una red TCP/IP, se considerarán los medios sobre cómo prevenir la red de posibles ataques.

1.1 Inserción de sistemas Cortafuegos

Los Cortafuegos (en inglés Firewalls), son dispositivos o sistemas que controlan el flujo de tráfico entre dos o más redes [12]**. Estos emplean métodos y políticas de seguridad. Básicamente son dispositivos cuya funcionalidad se limita a permitir o bloquear el tráfico entre dos redes en base a una serie de reglas y establecer el paso de la comunicación de una red a otra mediante el control de los protocolos TCP/IP. Su complejidad reside en las reglas que admiten y en cómo realizan la toma de decisiones en base a dichas reglas** [12]**.**

Estos sistemas actúan como una barrera central para reforzar el control de acceso a los servicios que se ejecutan tanto en el interior como en el exterior de la red. El Cortafuego intentará prevenir los ataques del exterior contra las máquinas internas de una red, denegando intentos de conexión desde partes no autorizadas [12]**. De éste modo, cualquier dispositivo utilizado como mecanismo de control de acceso a nivel de red para proteger a una red en concreto o a un conjunto de redes, podría ser representado como un sistema Cortafuegos.**

A la hora de instalar y configurar un sistema Cortafuegos, se debe considerar lo siguiente:

- **Todo tráfico que sale del interior hacia el exterior de la red que se desea proteger, debe pasar por el Cortafuego. Esto puede ser establecido bloqueando físicamente todo el acceso al interior de la red a través del sistema.**

- **Solo el tráfico de servicios autorizados podrá traspasar los filtros establecidos (el cual está definido en las políticas de seguridad locales del sistema).**

- **El propio Cortafuego debe estar protegido contra posibles intrusiones. Esto implica el uso de un sistema operativo de confianza con suficientes garantías de seguridad.**

En la figura N° 3.1, se puede apreciar como se establece un Cortafuegos:

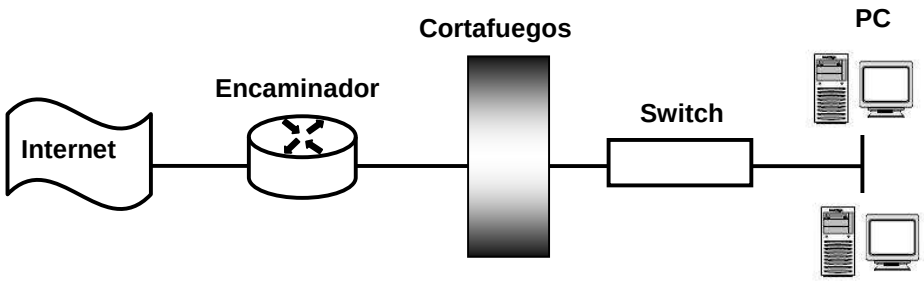


Figura N° 3.1 – Configuración Sistema Cortafuegos

1.2 Optimización de los sistemas Cortafuegos

Un sistema Cortafuego consta de Software y Hardware. El Software, puede ser cualquiera algoritmo que permita establecer las reglas en la transmisión de la información por la Red (filtrar). Un factor importante que permitirá cumplir la función del Software, será el Hardware asociado a dicho Software, de éste modo se realizará una sincronización entre máquina y programa que permitirá cumplir la función esencial y óptima del Cortafuegos.

Para una mayor optimización de los Cortafuegos, es necesario tener en conocimiento las formas y los componentes en que puede ser establecido éste tipo de sistemas, los que permitirán tener el primer nivel de seguridad de la Red a nivel de la Capa de Red del Modelo TCP/IP.

1.2.1 *Encaminadores con Filtrado de Paquetes*

Los Encaminadores (en Inglés Routers), son dispositivos que encaminan el tráfico TCP/IP bajo una serie de reglas de filtrado que deciden qué paquetes son guiados a través del Encaminador y qué paquetes no [3]**.**

En la figura N° 3.2 se puede apreciar un esquema general del filtrado que se realiza en una red implementando un sistema Cortafuego de filtrado de paquetes:

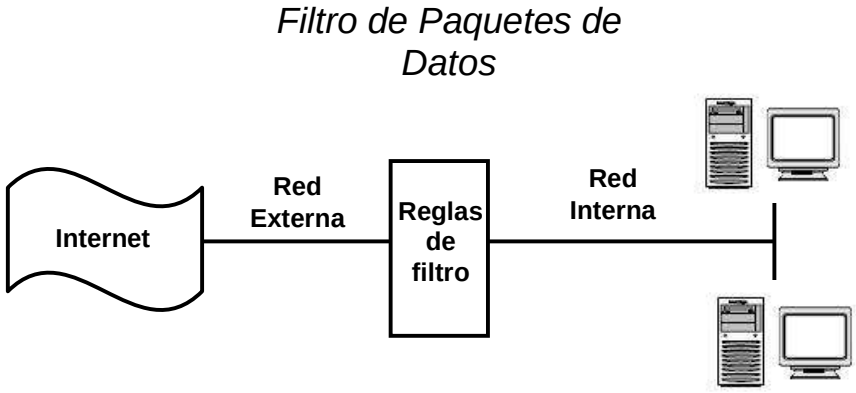


Figura N° 3.2 – Esquema General de un sistema Cortafuegos Con Filtrado de Paquetes

Las reglas de filtrado se encargan de determinar si a un paquete le está permitido pasar de la parte interna de la red a la parte externa y viceversa, verificando el tráfico de paquetes legítimo entre ambas partes. De ésta forma los Encaminadores con filtrado de paquetes, al trabajar a nivel de red, pueden aceptar o denegar paquetes analizando las cabeceras de los Datagramas. En primera instancia, las siguientes condiciones pueden ser encontradas:

- **Direcciones de origen y de destino.**
- **Tipos de protocolo e indicadores especiales (flags).**
- **Puertos de origen y de destino o tipos de mensaje (según el protocolo).**
- **Contenido de los paquetes.**
- **Tamaño del paquete.**

Es así como se comienzan a establecer las reglas de filtrado que permitirán manejar el control de acceso a la red.

Filtro de Paquetes de Datos

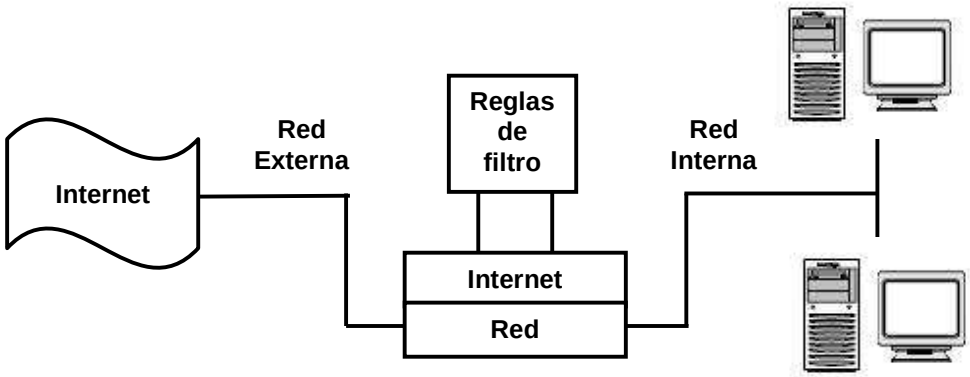


Figura N° 3.3 – Reglas de filtrado de Paquetes

Estas reglas estarán organizadas en conjuntos de listas (registros) con una determinada política por defecto (denegarlo todo, aceptarlo todo).

Cada paquete que llegue al dispositivo, será comparado con las reglas, comenzando por el principio de la lista hasta que se encuentre la primera coincidencia. Si hay coincidencia, la acción que realizará será de aprobación, por lo tanto la regla de confirmación será activada (denegar, aceptar, redirigir).

De otra forma, sino se verifica ninguna similitud, será consultada la política por defecto para saber que acción hay que tomar (dejar pasar el paquete, descartarlo, redireccionarlo). Si se trata de una política de denegación por defecto, en el caso que no sea encontrada ninguna coincidencia con el paquete, éste será descartado.

En una política de denegación, por defecto el administrador indica explícitamente todos los servicios que tienen que permanecer abiertos (los demás, por defecto, serán denegados en su totalidad) [3]**.**

En una política de aceptación, por defecto, las condiciones son más sencillas de administrar, pero incrementa el riesgo de permitir ataques contra nuestra red, ya que requiere que el administrador indique explícitamente qué paquetes son necesarios descartar (los demás, por defecto, serán aceptados en su totalidad).

A continuación se podrá apreciar un ejemplo de configuración en base al método de filtrado de paquetes:

En la figura N° 3.4 se presenta una red en la que s e ha implantado la siguiente política de seguridad mediante la configuración de un conjunto de reglas de filtrado de paquetes aplicadas en el mismo Encaminador:

- **Todos los sistemas de la red interna 10.0.0.0 pueden acceder a cualquier servicio TCP de Internet.**

- **El tráfico ICMP sólo está permitido de salida, no de entrada (para evitar la extracción de información mediante este protocolo).**

- **Los sistemas externos no se pueden conectar a ningún sistema interno, excepto al servidor de HTTP (10.0.0.1).**

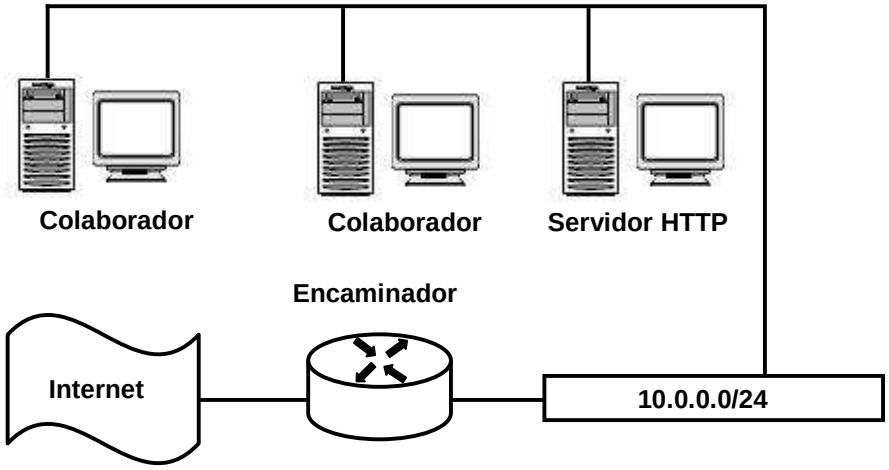


Figura N° 3.4 – Ejemplo 1 en Políticas de Seguridad en las Reglas de Filtrado de Paquetes

Las reglas de filtrado establecidas pueden ser vistas en la siguiente tabla, en base a cantidad de reglas, la acción, la dirección de origen y destino, el puerto asociados a la acción y la descripción de la acción:

Regla	Acción	Origen	Puerto de origen	Destino	Puerto de destino	Indicador	Descripción
1	Permite	10.0.0.0	-	-	-	ICMP	Permite Trafico ICMP de salida
2	Permite	10.0.0.0	-	-	-	TCP	Permite Conexiones TCP de salida
3	Permite	-	-	10.0.0.1	-	TCP	Permite Conexiones HTTP de entrada
4	Permite	-	-	10.0.0.0	80	-	Rechaza cualquier intento de conexión a la Red interna

Tabla N° 3.1 – Reglas de Filtrado Ejemplo 1

Como segundo ejemplo, podemos pensar en la misma red, pero con la siguiente política de seguridad:

- **Todos los sistemas de la red interna 10.0.0.0 pueden acceder a cualquier servicio TCP de la red Internet, excepto HTTP.**

- **Se deben de autorizar accesos al servidor de DNS (10.0.0.3).**

- **Los sistemas externos no se pueden conectar a ningún sistema interno, excepto al servidor de HTTP (10.0.0.1) y de SMTP (10.0.0.2).**

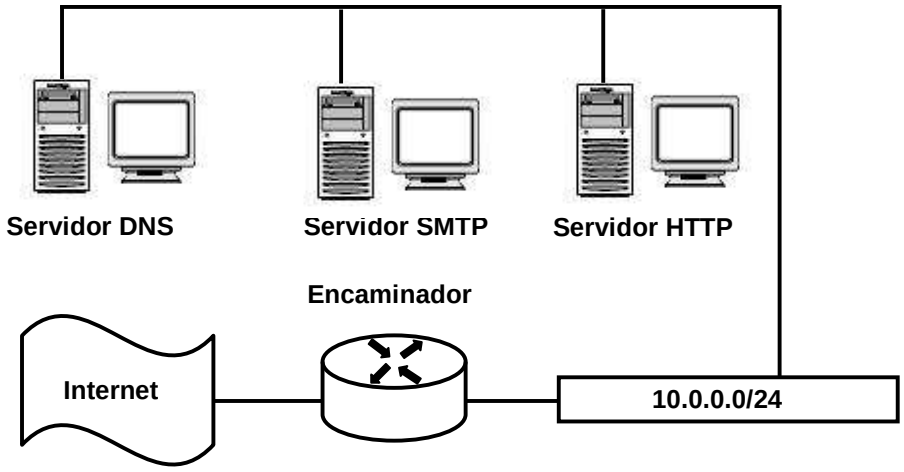


Figura N° 3.5 – Ejemplo 2 de Políticas de Seguridad en las Reglas de Filtrado de Paquetes

Las reglas de filtrado establecidas pueden ser vistas en la siguiente tabla, de acuerdo a las condiciones vistas anteriormente:

Regla	Acción	Origen	Puerto de origen	Destino	Puerto de destino	Indicador	Descripción
1	No Permite	10.0.0.0	-	-	80	TCP	No Permite conexiones a servidores HTTP
2	Permite	10.0.0.0	-	-		TCP	Permite Conexiones TCP de Salida
3	Permite	-	-	10.0.0.1	80	TCP	Permite Conexiones HTTP Entrantes
4	Permite	-	-	10.0.0.2	25	TCP	Permite Conexiones SMTP Entrantes
5	Permite	-	-	10.0.03	53	UDP	Permite Conexiones DNS Entrantes
6	No Permite	-	-	10.0.0.0	-	-	No Permite Conexiones a la Red Interna

Tabla N° 3.2 – Reglas de Filtrado Ejemplo 2

La construcción de un sistema Cortafuegos utilizando como componente un Encaminador con filtrado de paquetes, es de un acceso y administración no tan complejo. Además, ofrece un alto rendimiento para redes con una carga de tráfico elevada, permitiendo la implantación de la mayor parte de las políticas de seguridad establecidas.

Las políticas de seguridad, son el resultado de documentar las expectativas de seguridad, intentando plasmar en el mundo real los conceptos abstractos de seguridad. Se pueden definir de forma procesal (plasmando de forma práctica las ideas o filosofías de la empresa en cuanto a seguridad) o de manera formal (utilizando un modelo matemático que intente abarcar todos los posibles estados y operaciones).

1.2.2 *Encaminadores con filtrado de paquetes Dinámicos*

Los componentes de filtrado dinámico de paquetes, surgen como necesidad de proporcionar mecanismos efectivos de seguridad sobre el tráfico UDP. Éste tipo de componentes se asocian al tráfico UDP con

conexiones virtuales [12]**. Si un paquete de respuesta se genera y envía de vuelta al peticionario original, se establece una conexión virtual y se permite al futuro paquete de respuesta atravesar el Cortafuegos. La información asociada a una conexión virtual se guarda durante un periodo de tiempo muy corto, si no se recibe dicho paquete de respuesta durante éste, la conexión es invalidada. Algunos modelos de Cortafuegos, utilizando este tipo de componente, pueden realizar controles sobre el protocolo ICMP** [6]**.**
Por lo tanto, éste tipo de sistema se comporta exactamente igual al de los de filtrado simple de paquetes, con las mismas ventajas e idénticos inconvenientes.

1.2.3 ***Pasarelas a nivel de Aplicación***

Una Pasarela a Nivel de Aplicación, conocida también como servidor intermediario (En Inglés Proxy), no encamina paquetes a nivel de red sino que actúa como retransmisor a nivel de aplicación. Los usuarios de la red contactarán con el servidor intermediario, que a su vez estará ofreciendo un servicio Proxy asociado a una o más aplicaciones determinadas [12]**.**

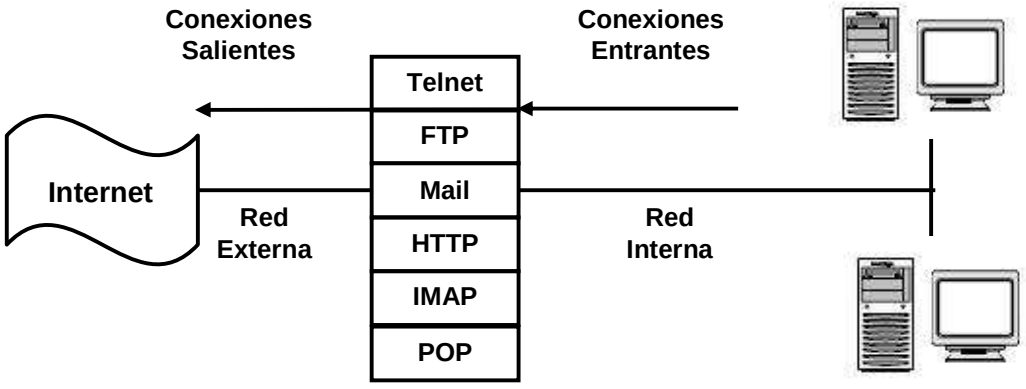


Figura N°3.6 – Pasarelas a Nivel de Aplicación

El servicio Proxy se encargará de realizar las conexiones solicitadas con el exterior y, cuando reciba una respuesta, se encargará de retransmitirla al equipo que había iniciado la conexión. De ésta forma, el servicio Proxy ejecutado en la Pasarela, aplicará las normas para decidir si se acepta o se rechaza una petición de conexión.

Una Pasarela separa completamente el interior del exterior de la red, permitiendo la autenticación de los usuarios que realizan peticiones de conexión y el análisis de conexiones a nivel de aplicación.

Estas dos características, provocan que las pasarelas ofrezcan una mayor seguridad respecto a los filtros de paquetes, presentando un rango de posibilidades muy elevado.

En el caso de una gran carga de tráfico en la red, el rendimiento puede llegar a reducirse drásticamente.

Las Pasarelas y los dispositivos de red con filtrado de paquetes son complementarios. Así, estos dos sistemas se pueden combinar, proporcionando más seguridad y flexibilidad que si se utilizara solamente uno, como se muestra en la siguiente figura:

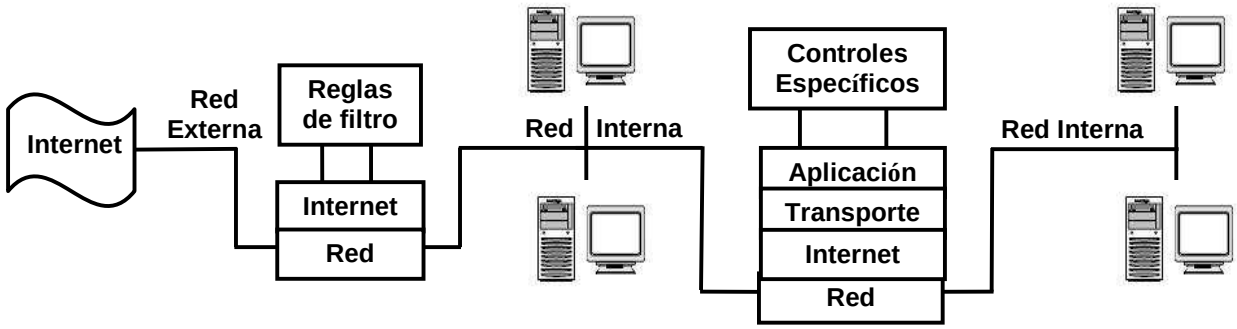


Figura N° 3.7 – Complemento de Filtro de Paquetes y Pasarelas a nivel de Aplicación

Cuando la Pasarela verifica al cliente, abre una conexión al servidor Proxy, siendo éste el responsable de transmitir los datos que reciba el cliente del servidor intermediario.

Éste funcionamiento particular provoca que las Pasarelas a nivel de aplicación, presenten un rendimiento inferior que los filtros de paquetes (debido al elevado número de conexiones adicionales que hay que realizar). Para evitar el bajo rendimiento, los servidores intermediarios se pueden configurar para realizar una copia de los datos recibidos de un sistema y entregarlos de nuevo más tarde si otro equipo de la red los solicita.

El uso de las Pasarelas permite el acceso únicamente a aquellos servicios para los que hay un servidor Proxy habilitado. Es así como una Pasarela contiene servicios intermediarios tan solo para los servicios HTTP y DNS, entonces sólo HTTP y DNS estarían permitidos en la red interna y el resto de servicios serían completamente rechazados.

También se debe considerar que, los servidores intermediarios pueden implantar el filtro de conexiones por dirección IP de la misma forma que los filtros de paquetes, ya que la dirección IP está disponible en el ámbito de aplicación en el cual se realizará el filtrado.

Aún obteniendo más control global sobre los servicios vigilados, las Pasarelas también presentan algunas problemáticas. Uno de los primeros inconvenientes que hay que destacar, es la necesidad de tener que configurar un servidor Proxy para cada servicio de la red que se debe vigilar (HTTP, DNS, Telnet, FTP). Además, en el caso de protocolos cliente servidor, como por ejemplo FTP, pueden llegar a ser necesarios algunos pasos adicionales para conectar el punto final de la comunicación.

1.2.4 *Pasarelas a nivel de circuito*

Las Pasarelas a nivel de circuito, son un híbrido entre los esquemas de filtrado de paquetes y el uso de servidores intermediarios. Una Pasarela a nivel de circuito es un dispositivo similar al de Pasarela a nivel de aplicación,

donde el usuario establece primero una conexión con el sistema Cortafuegos y este establece la conexión con el equipo de destino.

Una Pasarela a nivel de circuito, opera de manera similar a un filtro de paquetes a nivel de red, una vez que la conexión ha sido inicializada. Así, una vez establecida la conexión, el dispositivo se encargará de retransmitir todo el tráfico entre ambas partes sin inspeccionar el contenido de los paquetes a nivel de aplicación, tal y como muestra la siguiente figura:

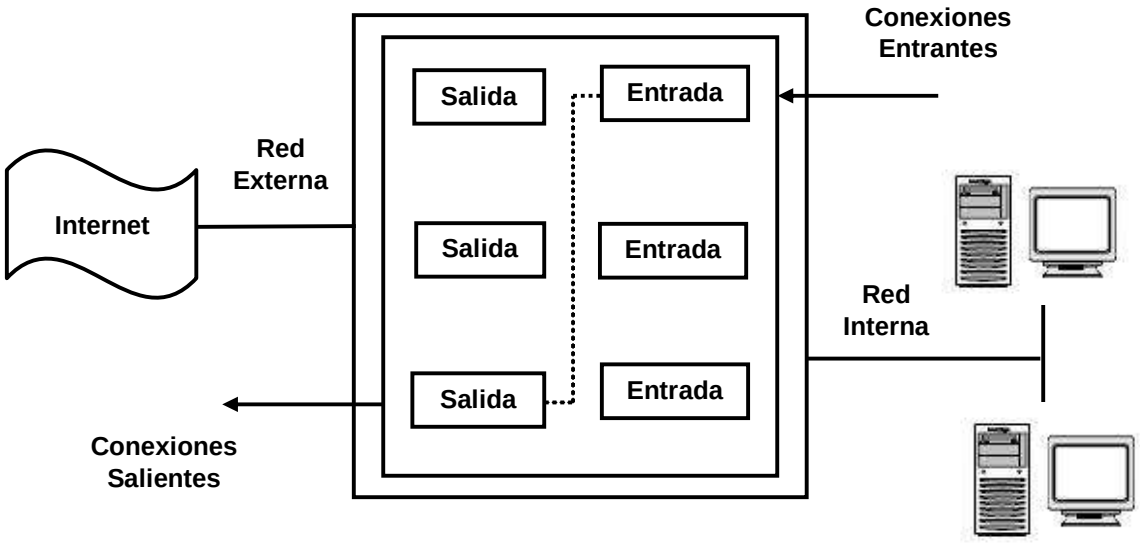


Figura N°3.8 – Pasarela a Nivel de Circuito

La función de seguridad que ofrece éste tipo de dispositivo, consiste en determinar qué conexiones están permitidas, antes de bloquear conexiones hacia el exterior.

Esta forma de trabajar es mucho más rápida que un sistema tradicional, ya que las conexiones pueden ser restringidas a nivel de usuario sin necesidad de analizar todo el contenido de los paquetes transmitidos.

1.2.5 *Inspección de condiciones*

Este tipo de componente, reúne características de los tipos de componentes mencionados anteriormente. Filtra paquetes según las direcciones de origen y de destino y los números de puerto. También controla los indicadores SYN y ACK y los números de secuencia de forma análoga a los dispositivos de acceso a nivel de circuito [12]**, por último, cataloga el contenido de los paquetes a nivel de aplicación. Frecuentemente ofrece mejor rendimiento a los Cortafuegos que los tipos de componentes mencionados anteriormente. La configuración del Cortafuegos, utilizando esta componente, actúa a nivel de red en el modelo TCP/IP.**

1.3 Tipos de Arquitectura de los sistemas Cortafuegos

Los Cortafuegos se pueden configurar en diferentes arquitecturas, proporcionando diversos niveles de seguridad a diferentes costos de instalación y operación. Las organizaciones deberían hacer corresponder su perfil de riesgo con el tipo de arquitectura de Cortafuegos seleccionada.

Las principales arquitecturas de Cortafuegos son:

1.3.1 *Equipo Multi-Puerto*

Se trata de un equipo que tiene más de un interfase de red. Cada interfase se conecta a segmentos de red física y lógicamente separados. Un equipo de doble puerto (un computador con dos interfaces), es el ejemplo más común de equipo Multi-Puerto. Un Cortafuegos de doble puerto, es un Cortafuegos con dos tarjetas de red (NIC), cada interfase conectado a una red diferente [3]**. Por ejemplo, una interfase de red normalmente se conecta a la red externa no segura, mientras que el otro se conecta a la red interna o segura. En esta configuración, uno de los principios de seguridad clave es**

no permitir que el tráfico procedente de la red no segura, se encamine directamente a la red segura, el Cortafuegos siempre debe actuar como intermediario. El Encaminamiento del Cortafuegos se inhabilitará para un Cortafuegos de doble puerto para que los paquetes IP de una red no se encaminen directamente de una red a la otra.

1.3.2 *Equipo Pantalla*

Un Cortafuegos con esta arquitectura, utiliza un equipo denominado Bastión (En Inglés Bastion Host), para que todos los equipos de fuera se conecten, en vez de permitir conexión directa a otros computadores internos menos seguros [3]**.**

Un equipo bastión, es un sistema informático que ha sido fuertemente protegido para soportar los supuestos ataques desde un lugar hostil (en este caso, Internet) y que actúa como punto de contacto entre el interior y el exterior de una red.

Para realizar esto, un Encaminador de filtrado de paquetes se configura para que todas las conexiones a la red interna desde la red externa, se dirijan hacia el equipo Bastión. Si se utilizara un Cortafuegos de filtrado de paquetes, entonces un equipo Bastión debería establecerse para que todas las conexiones desde la red externa vayan a través del computador Bastión para impedir que la conexión sea directa a Internet entre la red de la organización y el mundo exterior.

1.3.3 *Subred Pantalla*

Esta arquitectura es esencialmente similar a la arquitectura del equipo pantalla, pero añade una capa extra de seguridad, creando una red en la que reside el equipo Bastión (denominada red perimetral), la cual se encuentra separada de la red interna. Una subred pantalla se crea añadiendo una red perimetral que separe la red interna de la externa. Esto asegura que si existe

un ataque con éxito en el equipo Bastión, el atacante está restringido a la red perimetral por el Encaminador de pantalla que se conecta entre la red interna y la red perimetral [3]**.**

1.4 Implementación de Zonas Desmilitarizadas (DMZ)

En ciertas instalaciones, no es suficiente un único dispositivo Cortafuegos. Aquellas redes formadas por múltiples servidores, accesibles públicamente desde el exterior, juntamente con estaciones de trabajo que deberían estar completamente aisladas de conexiones con el exterior, se beneficiarán de la separación entre dos grupos de sistemas Cortafuegos.

Se tiene el siguiente ejemplo de una red:

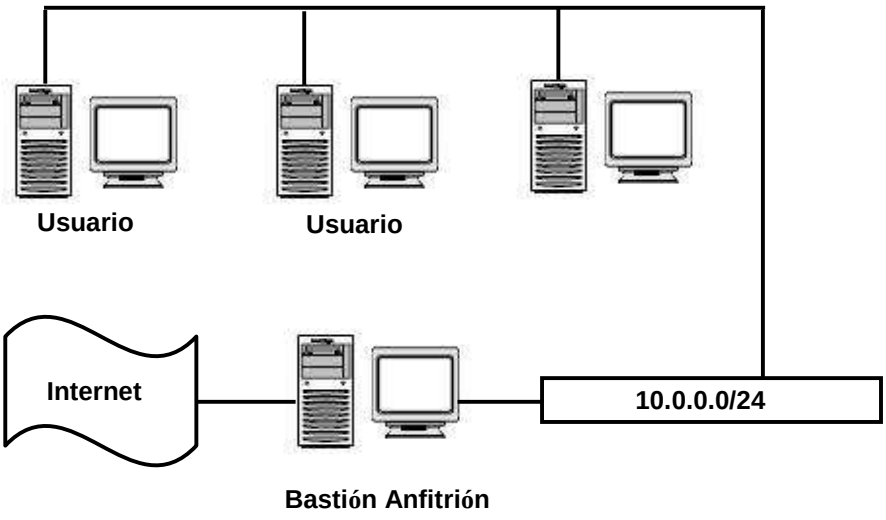


Figura N° 3.9 – Ejemplo de una

En la figura N° 4.9 se ve un único sistema Cortafue gos como punto de protección, implantado mediante la utilización de un equipo Bastión con una arquitectura Multi-Puerto.

La particularidad de la arquitectura Multi-Puerto, considera para establecer la zona Desmilitarizada [11]**, la construcción de un equipo Bastión que tenga la capacidad de encaminamiento desactivada. De ésta forma, los**

paquetes IP de un extremo de la red (la parte hostil) no serán encaminados hacia la parte protegida, y viceversa, a no ser que se indique lo contrario.

Mediante ésta arquitectura, los equipos de la red interna se pueden comunicar con el equipo Bastión, los equipos de la red externa pueden comunicarse con el equipo Bastión, pero los equipos de la red interna y externa no se pueden poner en comunicación directamente, sino que un servidor intermediario se encarga de realizar las conexiones en nombre de éstas dos partes.

Esto hace que la arquitectura Multi-Puerto sea un punto crítico en la seguridad de la red. Si un atacante consigue comprometer cualquiera de los servidores que se encuentre detrás de este punto único, las otras máquinas podrán ser atacadas sin ninguna restricción desde el equipo que acaba de ser comprometido.

Para prevenir éstas situaciones, es posible la utilización de dos dispositivos cortafuegos, introduciendo el concepto de Zona Desmilitarizada o DMZ.

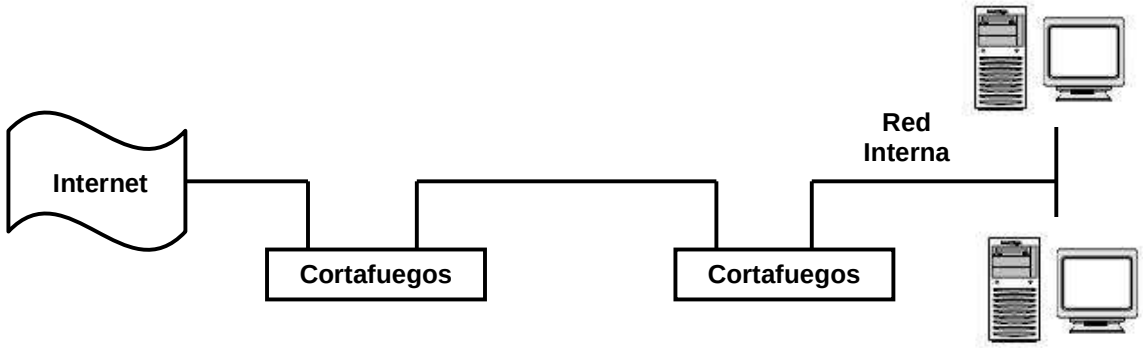


Figura N° 3.10 – Zona Desmilitarizada

En la figura N° 3.10 se puede apreciar un Cortafuegos que separa el exterior de la red del segmento desmilitarizado (DMZ) [11] **y los servidores que tienen que ser públicos desde el exterior de la red. Mientras el otro Cortafuegos que hace de punto de contacto entre la red interna y la Zona**

Desmilitarizada, se configurará para que rechace todos los intentos de conexión que vayan llegando desde el exterior. De éste modo, si un atacante consigue introducirse en uno de los servidores de la zona Desmilitarizada, será incapaz de atacar inmediatamente una estación de trabajo. Es decir, aunque un atacante se apodere del segmento de los servidores, el resto de la red continuará estando protegida mediante el segundo de los Cortafuegos.

1.4.1 Combinación de tecnologías para la construcción de una DMZ

En la figura N° 3.11, se puede ver el uso de un Enc aminador con filtrado de paquetes, juntamente con la utilización de un servidor intermediario para el establecimiento de una zona Desmilitarizada.

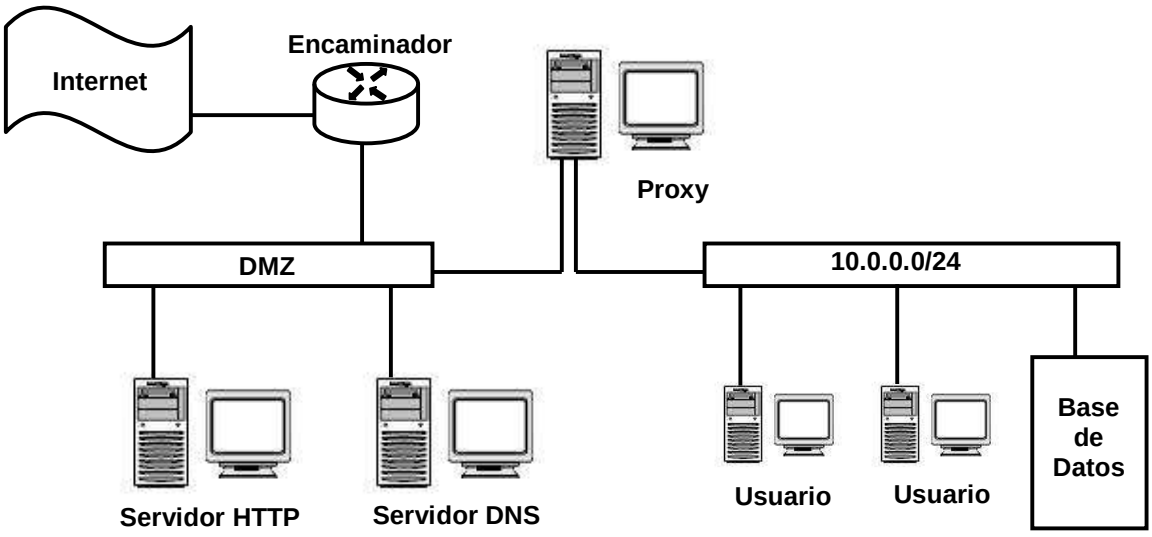


Figura N°3.11 – Combinación de Tecnologías usando DMZ

Otra forma de solucionar los mismos problemas planteados, consiste en la utilización de un sistema que implemente una inspección de estados en el filtro de paquetes. En la inspección de estados, se puede apreciar que el

rendimiento de los filtros de paquetes se combina con la seguridad adicional que presenta la utilización de servidores intermediarios.

De ésta forma, se puede simplificar el esquema planteado anteriormente y a la vez, mantener un nivel de rendimiento sin renunciar a las capacidades de monitoreo que ofrece la utilización de un punto de protección único.

En la figura N°3.12 se ilustra la implantación de un equipo Bastión con arquitectura Multi-Puerto y con implantación de inspección de estados.

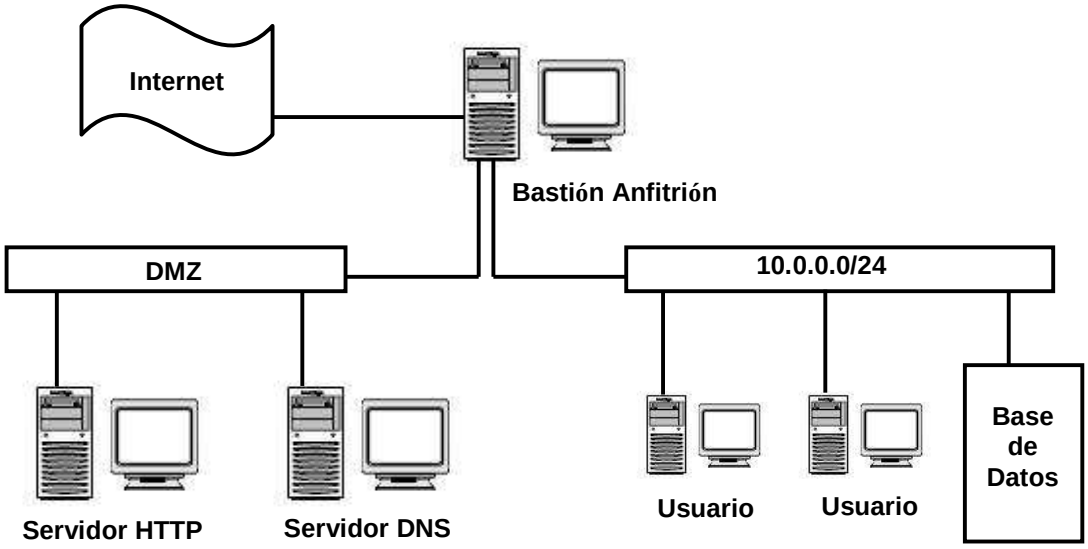


Figura N°3.12 – Arquitectura Multi-Puerto con uso de equipo Bastión

1.5 Características adicionales de los sistemas Cortafuegos

La utilización de sistemas Cortafuegos, permite establecer una barrera de control que mantendrá la red protegida de todos aquellos accesos no autorizados, actuando como un punto central de control y realizando las tareas de administración más simples.

No obstante, éste control y protección de la red, son únicamente una de las posibilidades que pueden ofrecer los sistemas Cortafuegos más modernos.

Los sistemas cortafuegos pueden ofrecer otras funciones adicionales a su uso [12]**, entre los cuales se pueden incluir:**

Filtrado de contenidos : Muchas organizaciones desean evitar que sus usuarios utilicen los recursos corporativos para navegar por determinados sitios Web no deseados.

El filtrado de contenidos ofrecido por algunos sistemas Cortafuegos, puede bloquear el acceso a estos sitios Web, a la vez que protege la red contra cualquier código malicioso insertado en sus páginas, como por ejemplo: ActiveX y código Java hostil.

Red Privada Virtual : Este tipo de red ofrecida por la mayoría de los sistemas Cortafuegos actuales, permite la construcción de un túnel seguro entre dos puntos de la red, normalmente para proteger las comunicaciones de una red corporativa al atravesar una red hostil (como es el caso de Internet).

Traducción de Direcciones de Red : Aunque no se trata estrictamente de una funcionalidad relacionada con la seguridad, la mayoría de los sistemas Cortafuegos ofrecen la posibilidad de realizar NAT y poder así, asociar direcciones IP reservadas a direcciones válidas. Un ejemplo podría ser la traducción de direcciones IP del rango 10.0.0.0/24 de una red privada para que salgan hacia Internet con la dirección IP pública 200.126.106.6.

Balanceo de la Carga : El balanceo de la carga es un mecanismo ofrecido por muchos sistemas Cortafuegos que permite segmentar el tráfico de una red de forma distribuida. Algunos sistemas

Cortafuegos ofrecen actualmente funcionalidades que pueden ayudar, por ejemplo, a distribuir tráfico FTP o HTTP de forma totalmente distribuida.

Tolerancia a Fallos : Las tolerancias a fallos son un mecanismo que ciertos sistemas Cortafuegos ofrecen para dar soporte a determinar tipos de fallos. Para ello, se configura el Cortafuegos para una utilización funcional de alta disponibilidad. En estas situaciones, la mayor parte de las estrategias incluyen la utilización de distintos sistemas Cortafuegos sincronizados, de manera que uno de los sistemas estará a la espera de que se produzca un fallo en el equipo original para ponerse en funcionamiento y sustituirlo.

Detección de Ataques e intrusiones : Gran parte de los sistemas Cortafuegos incorporan la capacidad de detectar exploraciones y ataques conocidos. Este mecanismo puede ser de gran ayuda para brindar una mayor seguridad a la red, sin embargo, la funcionalidad de ésta detección puede presentar una sobrecarga operacional en el sistema Cortafuego, impidiendo sacar un máximo rendimiento y obstaculizando la función principal para la cual fue configurado el Cortafuegos.

Autentificación de Usuarios : Dado que el sistema Cortafuegos es un punto de entrada a la red, puede llevar a cabo una autentificación adicional a la que efectúan los servicios ofrecidos por la misma. Es así como la autentificación de usuarios en un sistema Cortafuegos tendrá la finalidad de permitir o rechazar la conexión al usuario que solicita una conexión con un servicio interno (normalmente, mediante un mecanismo más fuerte que el implantado por el servicio al que se conecta).

La construcción de servicios adicionales en un sistema Cortafuegos puede favorecer la red o puede ocasionarle inconvenientes si se realiza en

una forma equivocada. Si se realiza más de un servicio adicional, puede ocasionar una lentitud o dificultades al comprobar entre un servicio y otro.

2 *VULNERABILIDADES DE LOS SISTEMAS CORTAFUEGOS*

Los cortafuegos ofrecen excelente protección contra las amenazas a la red, pero no son una solución de seguridad total. Ciertas amenazas están fuera del control del Cortafuegos. Debe encontrar otras formas de protegerse contra ellas incorporando seguridad física, seguridad para anfitrión y educación para el usuario en su plan general de seguridad primaria.

2.1 Vulnerabilidades provocadas de forma interna

Un Cortafuegos puede evitar que un usuario del sistema envíe información del propietario fuera de la organización a través de su conexión de red, esto también se evitaría no teniendo ninguna conexión con la red externa. Pero ese mismo usuario podría copiar los datos en disco o papel y sacarlos del edificio.

Los usuarios internos pueden robar datos, dañar el Hardware y el Software y modificar los programas sin acercarse al Cortafuegos. Las amenazas desde dentro requieren medidas de seguridad internas [3]**.**

2.2 Vulnerabilidad de conexiones sin pasar por Cortafuegos

Un Cortafuegos puede controlar el tránsito que pasa a través de él de manera eficaz, sin embargo, no hay nada que pueda hacer con el tránsito que no pasa por él. Es así como el Cortafuegos no puede proteger la red con los accesos telefónicos conmutados si éstos están detrás del Cortafuegos.

2.3 Vulnerabilidad frente a amenazas desconocidas

Un Cortafuegos está diseñado para proteger contra amenazas conocidas. Uno bien diseñado puede proteger también contra nuevas amenazas (al negar todos los servicios menos los confiables, un cortafuegos evita que las personas instalen servicios nuevos e inseguros). Sin embargo, ningún Cortafuegos puede defenderse de manera automática contra cada amenaza nueva que surge [3]**. No puede instalar un Cortafuegos una sola vez y esperar que lo proteja para siempre, hay que mantenerlo y actualizarlo.**

2.4 Vulnerabilidades a Nivel de Software

Los cortafuegos no pueden mantener los Software maliciosos (viruses) de los equipos fuera de la red. Aunque muchos Cortafuegos revisan todo el tránsito que entra para determinar si puede pasar a la red interna, la exploración ocurre en su mayoría a nivel direcciones fuente, destino y números de puerto, no en los detalles de los datos. Aún cuando se tenga filtrado de paquetes o Software Proxy complejo, la protección contra Software maliciosos en un Cortafuegos no es muy práctica. Hay demasiados tipos de Software maliciosos e infinidad de formas en que uno de ellos puede ocultarse dentro de los datos.

Detectar un Software malicioso al azar en un paquete de datos que pasa a través de un Cortafuegos es muy difícil [3]**, si de deseara realizar una inspección se necesitaría realizar un reconocimiento donde el paquete sea parte de un programa, determinando como debe verse el programa y analizando los cambios que éste pueda presentar debido alguna condición. Estos cambios pueden ser un indicador de que algo no está en orden de acuerdo al correcto funcionamiento de un Software determinado.**

3 *PROFUNDIZACIÓN EN LAS AMENAZAS DE LOS SISTEMAS CORTAFUEGOS*

El propósito de un Cortafuegos es proporcionar un punto de defensa y acceso controlado y auditado para servicios, tanto desde dentro como desde fuera de una red privada de una organización, permitiendo y/o denegando el flujo de paquetes a través del Cortafuegos.

Las amenazas de un Cortafuegos se pueden estructurar en categorías que permitirán tener un concepto mas especifico de los inconvenientes:

3.1 Amenazas Genéricas

Usuarios no autorizados pueden ganar acceso lógico al Cortafuegos, donde la clasificación para usuarios no autorizada se utiliza para cubrir todas aquellas personas que tienen o pueden intentar ganar acceso lógico al Cortafuegos, pero no tienen autoridad para ganar acceso lógico o realizar operaciones sobre su información [12]**.**

De éste mismo modo, éstos usuarios pueden llevar a cabo ataques de dirección de red desde una conexión de red a otra, atravesando el Cortafuegos. Aquí el Cortafuegos proporciona control de acceso entre una o más redes externas (no dignas de confianza) o internas (privadas, de confianza). La amenaza específica encontrada es que un sujeto de una red externa intente suplantar a un sujeto de la red interna. Es así como se pueden realizar ataques a los servicios y comenzar a ver amenazas que dependen de los protocolos que se permiten o deniegan a través del Cortafuegos.

A su vez se debe considerar la realización de ataques del tipo encaminamiento en el nivel de red, ya que los protocolos del nivel de red permiten al administrador de un paquete especificar el camino que el paquete va a seguir desde la fuente al destino.

Si el encaminamiento está indicado en la cabecera de protocolo, la función que procesa el protocolo se salta cualquier comprobación de reglas, de éste modo se ofrece un camino no deseado para cruzar por un túnel el Cortafuegos realizando una nueva función de encaminamiento.

Un usuario no autorizado puede intentar realizar muchas veces diferentes ataques contra una red a proteger, sino existe personal en la red atacada que se dé cuenta de que tales ataques están siendo realizados, le esta dando un factor libertad a este usuario de encontrar puntos o vacíos para acceder a la red interna.

Es allí donde puede faltar una revisión de registros de auditorías (conjunto de descripciones y datos de los mensajes de forma detallada). Si estos datos no llegaran a ser revisados de buena forma, ya sea la cantidad de datos generados o la falta de herramientas de revisión adecuadas, pueden favorecer a un atacante para no ser detectado mientras realiza intentos de penetración repetidos.

Si un atacante pudiera modificar el registro de auditoría, puede ocasionar algunos inconvenientes que permitirán modificar directamente el registro de auditoría manipulándolo a través de una interfase del Cortafuegos. Así también si se tiene acceso al registro, puede producirse un mal funcionamiento del Cortafuegos después de realizar una penetración o intento de penetración y si el registro de auditoría no está suficientemente protegido posiblemente puede perderse, de modo que se enmascaren las acciones del atacante.

Esto puede desencadenar problemas de carácter más sustancial y complejos que permitan modificar la configuración del Cortafuegos y otros datos de seguridad relevantes. Debido a ello, pueden ocurrir fallos de seguridad debido a defectos en el Cortafuegos. La seguridad ofrecida puede ser garantizada sólo hasta el punto de que todas las características de seguridad pueden ser confiables en cuanto a ser efectivas a la hora de contrarrestar las amenazas y operar correctamente y de forma fiable. Los agentes de amenazas pueden descubrir defectos en el Cortafuegos que

pueden trastornar de modo que el desarrollo de las funciones de seguridad se cambie para su provecho. Dicho trastorno del Cortafuegos puede ocurrir durante la entrega e instalación.

3.2 Amenazas aplicadas al entorno de Operación

En éste tipo de amenazas, se deben considerar ciertas condiciones ocasionadas por el entorno de la red, pudiendo ser falencias, falta de control por parte de los administradores, los cuales son responsables de establecer las reglas de control de acceso y de monitorizar el registro de auditoría.

Un ejemplo de éste tipo de amenaza, pueden ser realizadas por usuarios hostiles (usuario que desea perjudicar el funcionamiento de la red) de una red protegida (situados detrás del Cortafuegos) que desean compartir información con usuarios de la red externa. Esto puede ocasionar por parte de usuarios de una red interna (protegida) el envío de información de forma ilegítima a un usuario de una red externa [12]**.**

Esto puede ocasionar a una red una vulnerabilidad que permite atacar a equipos que son parte de la red protegida, ya que de acuerdo a lo analizado, un Cortafuegos sirve para proteger a los usuarios de una red interna de los usuarios externos a la red, no puede proteger de los ataques no dirigidos contra el Cortafuegos.

Es así como los usuarios hostiles de una red protegida pueden intentar realizar ataques sofisticados a los servicios y protocolos de alto nivel. Donde estos tipos de ataques eligen defectos de los niveles de protocolo (y servicios que utilizan dichos protocolos) por encima del nivel de transporte. Aquí el Cortafuegos puede ser capaz de denegar completamente paquetes a servicios específicos, pero una vez que a los paquetes se les permite pasar, entonces pueden ser posibles los ataques a los servicios que son elegidos, no necesitando la verificación del contenido del contenido del paquete.

3.3 Amenazas de acceso físico

El Cortafuegos y la consola asociada directamente conectada, es segura, es decir, el acceso se encuentra limitado sólo al personal autorizado, es así como solo el personal autorizado (administradores) interactúa con el Cortafuegos a través de consolas directamente conectadas, es decir, ningún sistema de entrada con nombre de usuario y clave (login). Por ello si un usuario hostil tuviera acceso a una consola del Cortafuegos puede configurar a su modo y ocasionar algún vacío en tan sólo unos minutos [12]**.**

4 *MÉTODOS DE MANTENIMIENTO DE UN SISTEMA CORTAFUEGOS*

El mantenimiento que se debe realizar a un Cortafuegos es un elemento que se debe considerar constantemente, ya que cada día se presentan inconvenientes que pueden alterar el funcionamiento de la red. Por ello es recomendable realizar revisiones y mantenciones cada cierto tiempo.

A continuación se detallaran 3 de los principales métodos de mantenimiento que se asocian a los sistemas Cortafuegos:

4.1 Mantenimiento General

Respaldo del Cortafuegos : Consiste en realizar un respaldo de todas las partes de un Cortafuegos, lo cual se refiere no sólo a los equipos de usos múltiples que puede estar usando como equipos Bastión o servidores internos, sino que también a los Encaminadores u otros dispositivos de propósitos especiales.

Por lo general, no es sencillo reconstruir configuraciones de Encaminadores, su seguridad depende de tenerlos bien configurados. A los equipos de usos múltiples se les debe colocar un sistema de copias de

respaldo automatizado de preferencia, que permita crear correos de confirmación cuando funcione de modo normal y mensajes completamente diferentes cuando detecte inconvenientes.

Administración de cuentas : El mantenimiento de las cuentas (agregar nuevas cuentas, quitar las viejas, caducar las contraseñas) es una de las tareas de mantenimiento que se descuidan con más frecuencia. Por ello en los sistemas Cortafuegos, es muy importante que las nuevas cuentas se agreguen correctamente, que las viejas se quiten con oportunidad y que las contraseñas se cambien de modo apropiado.

Administración del espacio en disco : El mantenimiento de la información siempre se extiende hasta llenar todo el espacio disponible, aun en equipos que casi no existen usuarios. Por lo general las personas que utilizan la red dejan cosas en rincones extraños del sistema, de manera provisional, y luego se quedan ahí, lo cual ocasiona más problemas de los que se imagina, ya que en algún momento se puede requerir ese espacio de disco. De esta forma, éste exceso de información puede alterar la respuesta del Cortafuegos en relación a la cantidad de memoria, provocando conflictos en la órdenes, demora en la ejecución.

4.2 Actualización de los Sistemas Cortafuegos

El mantenerse actualizado es un factor fundamental que permitirá conocer los problemas que se están presentando en los sistemas Cortafuegos, de ésta forma se podrá tomar un resguardo anticipado de la red y así mantener su rendimiento [3]**.**

Hay dos factores que permitirán tener un sistema actualizado, los cuales son:

Actualización por parte de los administradores : Los continuos avances en las condiciones de seguridad, los avances en el descubrimiento de nuevos errores, nuevos ataques, nuevas configuraciones o arreglos y nuevas herramientas; establecen un continuo aprendizaje y recopilación de información que permitirá tener en conocimiento los cambios que se presentan. De ésta forma los administradores deben recurrir a todas las instancias para obtener información (noticias, revistas, foros especialistas, etc.), y estar a la vanguardia de los sistemas Cortafuegos.

Mantención de los sistemas actualizados : Para mantener un sistema actualizado, se debe estudiar cualquier problema nuevo sobre el que se esté hablando. Por ello, los administradores deben ser capaces de solicitar información de las fuentes descritas en los sistemas que se han producido los inconvenientes para determinar si el problema que se presenta, representará un riesgo para su red en particular. Es así que se debe realizar una discriminación de los nuevos conceptos y un mejoramiento en base a los factores que pueden ocasionar problemas y los que no.

CAPITULO IV:

Condiciones de seguridad avanzadas para protección de una Red TCP/IP

1 *INSERCION CRIPTOGRAFICA PARA PROTEGER LA RED TCP/IP*

La protección de la información es un nivel de seguridad superior a la prevención mencionada en el capitulo número 3, es el siguiente movimiento a realizar si las formas de prevención fueron vulneradas.

Por ello para proteger la red y establecer su adecuada comunicación, se deberá involucrar un nuevo término a la seguridad de los datos el cual es la criptografía, esta herramienta permitirá evitar que alguien intercepte, manipule o falsifique los datos transmitidos [5]**. En si este nuevo termino tratara de establecer una adecuada confidencialidad en conjunto con los equipos de sincronización a nivel de red.**

1.1 Criptografía

La criptografía es una rama de la criptología (que se encarga del estudio de lo oculto) y termino asociado al criptoanálisis que permite estudiar el sistema de claves de acceso y del cifrado de los mensajes.

En si la criptografía es el conjunto de técnicas (entre algoritmos y métodos matemáticos) que resuelven los problemas de autenticidad, privacidad, integridad, no rechazo en la transmisión de la información, permitiendo así crear métodos de protección de la información [5]**. Es así como realiza el envío de información secreta, mediante transformación que sufre el mensaje, conocidas como cifrado, de esta forma la información que se requiere mantener en secreto, aunque un adversario consiga ver qué datos se están enviando, le serán completamente ininteligibles. Sólo el destinatario legítimo (a quien se envío la información) será capaz de realizar la transformación inversa, recuperar los datos originales necesarios para poder dar una interpretación a la información enviada.**

Cuando la protección que se desea obtener consiste en garantizar el secreto de la información, es decir, la confidencialidad, es donde se utiliza

el método criptográfico de cifrado, el que en si permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, utilizando variables numéricas, alfanuméricas, múlti-numéricas y múlti-alfanuméricas en cierto lenguaje bajo bases matemáticas, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

En la figura N° 4.1 se puede observar un ejemplo de un sistema implementando criptografía que nos muestra como sería el funcionamiento esquemático, sea cual sea el canal de transmisión, del cifrado y descifrado de un mensaje en su paso del transmisor al receptor.

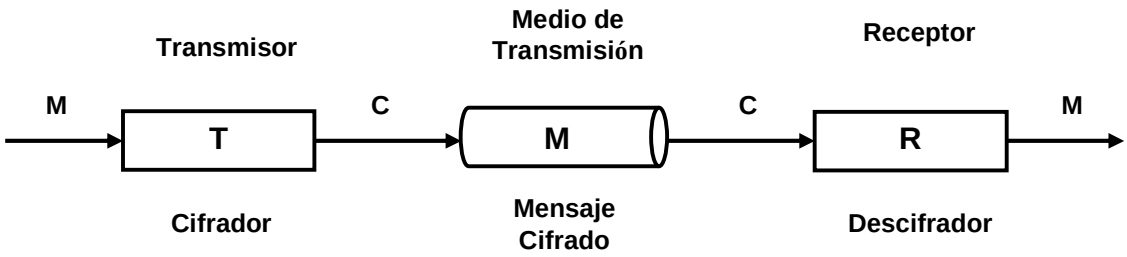


Figura N° 4.1 – Implementación de Criptografía

A continuación se puede ver un ejemplo:

Si *M* **es el mensaje que se desea proteger o texto en claro (Información que es de carácter ininteligible), cifrarlo consiste en aplicarle un algoritmo de cifrado** *f***, que lo transforma en otro mensaje que llamaremos texto cifrado** *C* **(documento que ha sido cifrado).**

De esta forma se tiene lo siguiente:

$$C = f(M)$$

Para que este cifrado sea útil, debe existir otra transformación o algoritmo de descifrado f^{-1}**, que permita recuperar el mensaje original a partir del texto cifrado:**

$$M = f^{-1}(C)$$

La criptografía se basa en la transposición y la sustitución con el objetivo de hacer algoritmos de cifrado complicados y rebuscados.

Es aquí donde comienza aparecer la inserción de sistema utilizando criptografía o criptosistemas que permitirán realizar una clasificación y formas con de cómo realizar la encriptación de los datos.

1.1.1 *Sistemas de cifrado simétrico*

Los sistemas de cifrado simétrico son aquellos que utilizan la misma clave para cifrar y descifrar un documento [5]**. 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. Este tipo de criptografía se conoce también como de clave privada o de llave privada.**

A la criptografía simétrica se le pueden aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar.

La representación básica de un tipo de sistema criptográfico simétrico puede ser apreciada en la siguiente figura:

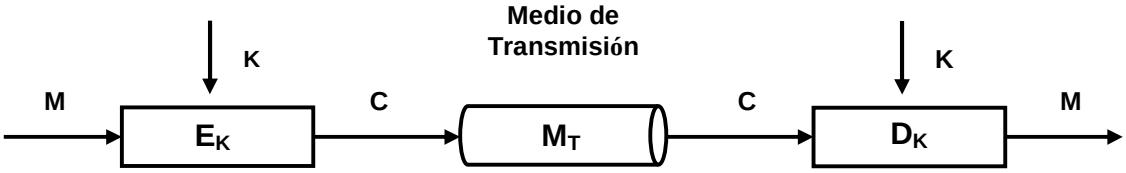


Figura N° 4.2 – Sistema de Criptográfico Simétrico

Con E_K se cifra el mensaje original aplicándole la clave *k* y con D_K se descifra, aplicándole de la misma forma la clave *k*.

La confidencialidad y la integridad se lograrán si se protegen las claves en el cifrado y en el descifrado. Es decir, se obtienen simultáneamente si se protege la clave secreta.

Según el tratamiento del mensaje y los algoritmos se puede catalogar a los sistemas de cifrado criptográfico simétricos de la siguiente forma:

1.1.1.1 *Cifrado en Bloques*

En un algoritmo de cifrado o descifrado que se aplica separadamente a bloques de entrada de longitud fija, y para cada uno de ellos el resultado es un bloque de la misma longitud [30]**.**

Para cifrar un texto en claro de *n* bits, se debe dividir en bloques de *a* bits cada uno y cifrar estos bloques uno a uno. Si *n* no es múltiple de *a*, se pueden agregar bits adicionales hasta llegar a un número lleno de bloques, pero luego puede ser necesario indicar de alguna forma cuántos bits había realmente en el mensaje original. El descifrado también se debe realizar bloque a bloque.

La figura N° 4.3 muestra el esquema básico del cifrado de bloque, donde *M* es el texto de mensaje, *k* la clave del mensaje y *C* el texto cifrado:

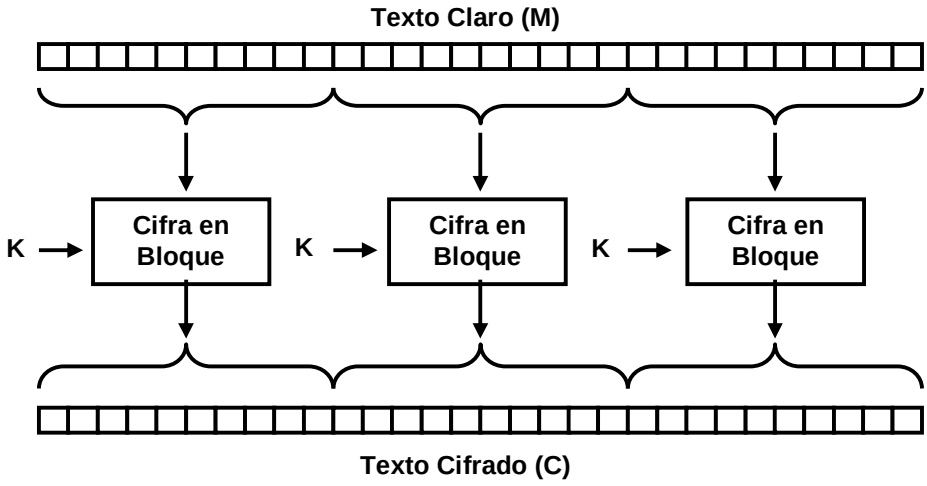


Figura N° 4.3 – Sistema de Cifrado en Bloques

Muchos de los algoritmos del cifrado de bloque se basan en la combinación de dos operaciones básicas, las cuales son:

La sustitución : Consiste en traducir cada grupo de bits de la entrada a otro, de acuerdo con una permutación determinada. Cada grupo de bits correspondería a una letra. De hecho, se trata de un caso particular de sustitución alfabética. En el caso más general, las letras del texto cifrado no tienen por qué estar a una distancia constante de las letras del texto en claro. La clave se puede expresar como la secuencia correlativa de letras que corresponden a la *A*, la *B*, la *C*, etc. Por ejemplo:

A B C D E F GHY J K LMNO P Q R S T UVWXY Z
Clave: *QWE R T YUYO P A S D F GH J K L Z X C V B NM*
Texto en claro: *A L E A J A C T A E S T*
Texto cifrado: *Q S T Q P Q E Z Q T L Z*

La transposición : Consiste en reordenar la información del texto en claro según un patrón determinado. Un ejemplo podría ser la formación de grupos de cinco letras, incluidos los espacios en blanco, y rescribir cada grupo (1, 2, 3, 4, 5) en el orden (3, 1, 5, 4, 2):

Texto en claro: *A L E A J A C T A E S T*
Texto cifrado: *E A A L C J A T A S T E*

La transposición por si sola no dificulta extraordinariamente el criptoanálisis, pero puede combinarse con otras operaciones para añadir complejidad a los algoritmos de cifrado.

El producto de cifras, o combinación en cascada de distintas transformaciones criptográficas, es una técnica muy efectiva para implementar algoritmos bastante seguros de forma sencilla. Por ejemplo, muchos algoritmos de cifrado de bloque se basan en una serie de repeticiones de productos sustitución-transposición.

De acuerdo a ello hay dos propiedades deseables en un algoritmo criptográfico las cuales son:

La confusión : Consiste en esconder la relación entre la clave y las propiedades estadísticas del texto cifrado, y la difusión, que propaga la redundancia del texto en claro a lo largo del texto cifrado para que no sea fácilmente reconocible.

La confusión consigue que, cambiando un solo bit de la clave, cambien muchos bits del texto cifrado.

La difusión : Implica que el cambio de un solo bit del texto en claro afecte también a muchos bits del texto cifrado.

En un bucle de productos de cifrados básicos, la sustitución contribuye a la confusión, mientras que la transposición contribuye a la difusión. La combinación de estas transformaciones simples, repetidas diversas veces, provoca que los cambios en la entrada se propaguen por toda la salida por efecto de desbordamiento.

A continuación se verán 3 de los más conocidos tipos de sistemas con cifrado en bloque:

1.1.1.1.1 *DES*

Este tipo de cifrado en bloques es un estándar en los sistemas de cifrado y lo que realiza es codificar en bloques de 64 bits del mensaje y este se somete a 16 interacciones (repeticiones), una clave de 56 bits. En la práctica el bloque de la clave tiene 64 bits, ya que a cada conjunto de 7 bits se le agrega un bit que puede ser usado como de paridad [24]**.**

El descifrado se realiza con la misma clave y los pasos inversos, lamentablemente este tipo de sistema ha sido vulnerado, debido a la posibilidades de desbloqueo de claves mediante software y que prueban

todas las combinaciones posibles con computadores de un alto rendimiento y proceso, sin embargo, esto fue solucionado implementando sistemas que implementan la base de DES pero con nuevas condiciones. Es así como se presenta uso de sistemas con un Doble DES (ejecuta el DES 2 veces con 3 claves distintas) y el Triple DES (2 claves y 3 etapas) [5]**.**

Por ello entonces la seguridad de los sistemas de clave simétrica pasa por la longitud de la clave de descifrado.

Dependiendo de la naturaleza de la aplicación DES tiene cuatro modos de operación para poder implementarse:

<u>Modo ECB</u> : (Electronic Codebook) es el más simple, y consiste en dividir el texto en bloques y cifrar cada uno de ellos de forma independiente [5]**.**

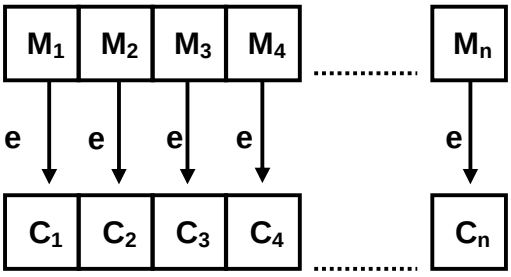


Figura N° 4.4 – Modo ECB

<u>Modo CBC</u> : (Cipher Block Chaining), Se suma a cada bloque de texto en claro, antes de cifrarlo, (bit a bit, con XOR) el bloque anteriormente cifrado.

Al primer bloque se le suma un vector de inicialización (VI), que es un conjunto de bits aleatorios de la misma longitud que un bloque. Escogiendo vectores distintos cada vez, aun que el texto en claro sea el mismo, los datos cifrados serán distintos. El receptor debe conocer el valor del vector antes de empezar a descifrar, pero es necesario falta guardar este valor en secreto, sino que normalmente se transmite como cabecera del texto cifrado [5]**.**

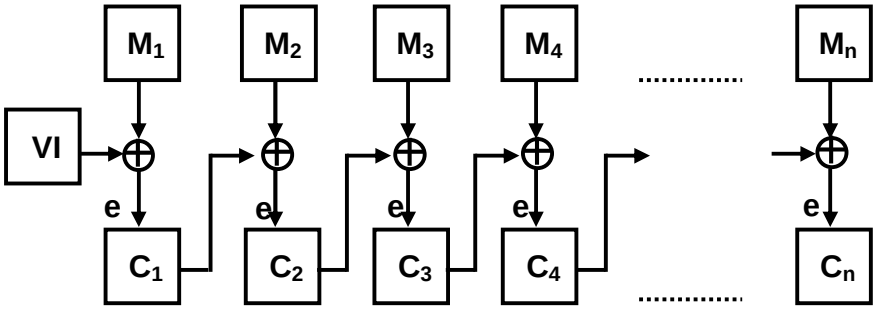


Figura N° 4.5 – Modo de Operación CBC

<u>Modo CFB</u> : (Cipher Feedback) El algoritmo de cifrado no se aplica directamente al texto en claro sino a un vector auxiliar (inicialmente igual al VI). Del resultado del cifrado se toman *n* bits que se suman a *n* bits del texto en claro para obtener *n* bits de texto cifrado. Estos bits cifrados se utilizan también para actualizar el vector auxiliar. El número *n* de bits generados en cada repetición puede ser menor o igual que la longitud de bloque *b*. Tomando como ejemplo *n* = 8, tenemos un cifrado que genera un byte cada vez sin que sea necesario esperar a tener un bloque entero para poderlo descifrar.

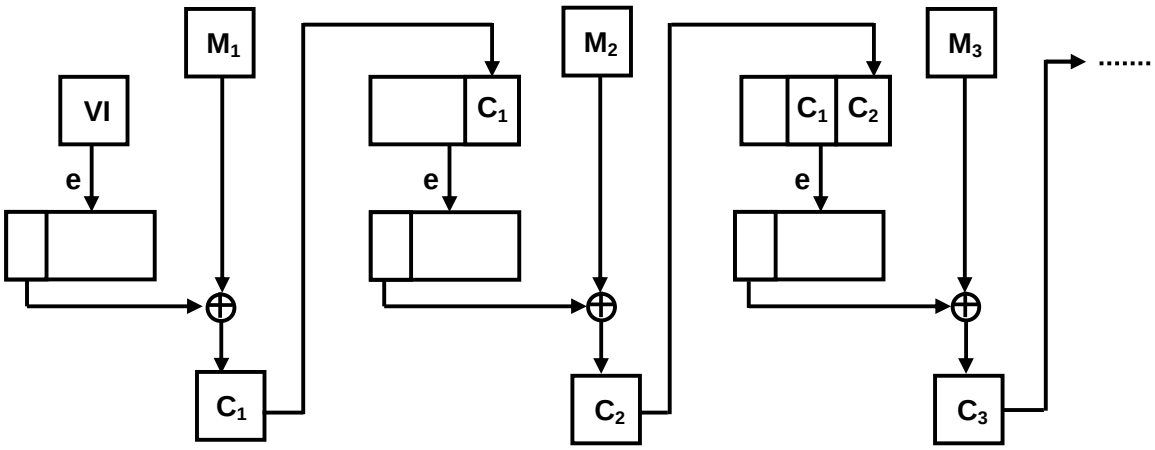


Figura N° 4.6 – Modo de Operación CFB

<u>Modo OFB</u> : (Output Feedback) Opera como el CFB pero en lugar de actualizar el vector auxiliar con el texto cifrado, se actualiza con el resultado obtenido del algoritmo de cifrado. La propiedad que distingue este modo de los demás consiste en que un error en la recuperación de un bit cifrado afecta solamente al descifrado de este bit.

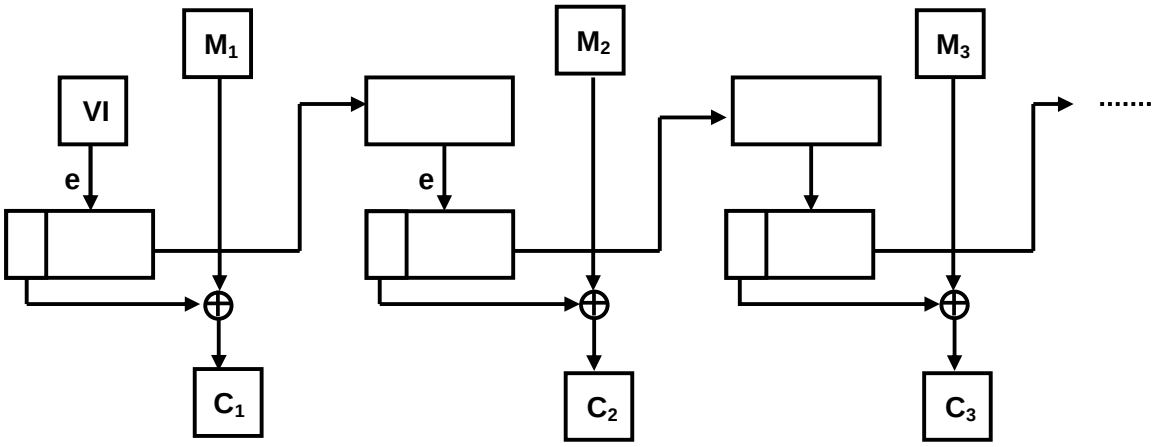


Figura N° 4.7 – Modo de Operación OFB

A partir de los modos anteriores se pueden definir varias variantes. Por ejemplo, el modo CTR (Counter) es como el OFB, pero el vector auxiliar no se realimenta con el cifrado anterior sino que simplemente es un contador que se va incrementando.

1.1.1.1.2 *<u>IDEA</u>*

Este tipo de cifrado en bloques trabaja con bloques de texto de 64 bits y con una clave de 128 bits con 8 iteraciones (8 repeticiones de instrucciones) y su descifrado se realiza aplicando el mismo algoritmo, pero con ciertos cambios y subclaves diferentes asociadas al mensaje original [5]**.**

1.1.1.1.3 *RSA*

Este tipo de cifrado se basa en la dificultad de factorizar números grandes por parte de poderosos equipos, con una gran capacidad de proceso de datos (alto rendimiento) [5]**. Su funcionalidad, rapidez de ejecución y fuerte estructura de base (Exponentes modulares y módulos fijos), hacen al cifrado RSA uno de los más utilizados, es por ello que a continuación se representara la estructura general de cómo se crean las claves por medio de este sistema:**

- **Se buscan dos números primos lo suficientemente grandes:** p **y** q **(de entre 100 y 300 dígitos).**
- **Se obtienen los números** $n = p \bullet q$ **y** $X = (p-1) \bullet (q-1)$**.**
- **Se busca un número** e **tal que no tenga múltiplos comunes con** X**.**
- **Se calcula** $d = e^{-1} \bmod X$**, con mod = resto de la división de números enteros.**

Ya con estos números obtenidos, n **es la clave pública y** d **es la clave privada. Los números** p**,** q **y** X **se destruyen. También se hace público el número** e**, necesario para alimentar el algoritmo.**

El cálculo de estas claves se realiza en secreto en la máquina en la que se va a guardar la clave privada, y una vez generada ésta conviene protegerla mediante un algoritmo criptográfico simétrico.

1.1.1.2 *Cifrado en Flujos*

El funcionamiento de un cifrado en flujo consiste en la combinación de un texto en claro M **con un texto de cifrado** S **que se obtiene a partir de la**

clave simétrica *k*. Para descifrar, sólo se requiere realizar la operación inversa con el texto cifrado y el mismo texto de cifrado.

En los esquemas de cifrado en flujo, el texto en claro *M* puede ser de cualquier longitud, y el texto de cifrado *S* ha de ser como mínimo igual de largo. De hecho, no es necesario disponer del mensaje entero antes de empezar a cifrarlo o descifrarlo, ya que se puede implementar el algoritmo para que trabaje con un flujo de datos que se va generando a partir de la clave (el texto de cifrado).

De ahí procede el nombre de este tipo de algoritmos. La siguiente figura ilustra el mecanismo básico de su implementación:

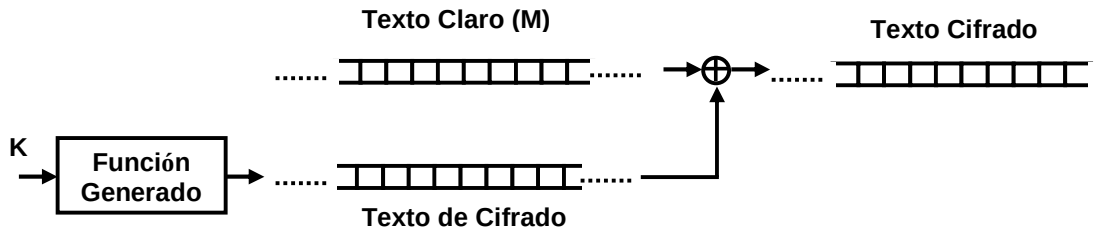


Figura N° 4.8 – Esquema de Cifrado y Descifrado en Flujo

1.1.1.3 *Cifrado síncrono y asíncrono*

Considerando el item anterior, si el texto de cifrado *S* depende exclusivamente de la clave *k*, se dice que el cifrado es síncrono. Este cifrado tiene el problema de que, si por algún error de transmisión, se pierden bits (o llegan repetidos), el receptor se desincronizará y sumará bits del texto *S* con bits del texto cifrado *C* que no corresponden, con lo cual el texto descifrado a partir de entonces será incorrecto. Esto se puede evitar con el cifrado asíncrono (auto sincronizante), en el cual el texto *S* se calcula a partir de la clave *k* y el mismo texto cifrado *C*. Es decir, en lugar de realimentarse con sus propios bits de estado, el generador se realimenta con los últimos *n* bits cifrados transmitidos. De este modo, si se pierden *m* bits consecutivos en la

comunicación, el error afectará como máximo al descifrado de *m*+*n* bits del mensaje original.

1.1.1.4 *Cifrados de funciones de dispersión unidireccional*

Este tipo de algoritmos también llamado funciones Hash seguras (Cadena de bits, de longitud predeterminada, que se obtiene a partir de una secuencia de bits de longitud arbitraria, como resumen de esta secuencia), permiten obtener una cadena de bits de longitud fija [5]**, relativamente corta, a partir de un mensaje de longitud arbitraria:**

$$H = h(M)$$

Para mensajes *M* iguales, la función *h* debe dar resúmenes *H* iguales. Pero si dos mensajes dan el mismo resumen *H* no deben ser necesariamente iguales.

Esto es así porque sólo existe un conjunto limitado de posibles valores *H*, ya que su longitud es fija, y en cambio puede haber muchos más mensajes *M* (si la longitud puede ser cualquiera, habrá infinitos).

Estas propiedades permiten el uso de las funciones Hash seguras para dar un servicio de autenticidad basado en una clave secreta *s* compartida entre dos partes *A* y *B*. Aprovechando la unidireccionalidad que poseen la funciones Hash, cuando *A* quiere mandar un mensaje *M* a *B* puede preparar otro mensaje M_s.

Para comprobar la autenticidad del mensaje recibido, *B* verifica que el resumen corresponda efectivamente a M_s. Si es así, quiere decir que lo ha generado alguien que conoce la clave secreta *s* (que debería ser *A*), y también que nadie ha modificado el mensaje.

Para verificar la autenticidad se debe recuperar el resumen enviado, descifrándolo con la clave secreta *s*, y compararlo con el resumen del mensaje *M*. Si un atacante que quisiera modificar el mensaje sin conocer la

clave podría intentar sustituirlo por otro que diera el mismo resumen, con lo cual *B* no detectaría la falsificación. Pero si la función de resumen es resistente a colisiones, esto le sería imposible al atacante.

Para dificultar los ataques contra las funciones de resumen, por un lado los algoritmos tienen que definir una relación compleja entre los bits de entrada y cada bit de salida. Por otro lado, los ataques por fuerza bruta se contrarrestan alargando lo suficiente la longitud del resumen. Por ejemplo, los algoritmos usados actualmente generan resúmenes de 128 ó 160 bits. Esto quiere decir que un atacante podría tener que probar del orden de 2128 o 2160 mensajes de entrada para encontrar una colisión (es decir, un mensaje distinto que diera el mismo resumen).

El esquema de la mayoría de funciones Hash usadas actualmente es parecido al de los algoritmos de cifrado de bloque, el mensaje de entrada se divide en bloques de la misma longitud, y a cada uno se le aplica una serie de operaciones junto con el resultado obtenido en el bloque anterior. El resultado que queda después de procesar el último bloque es el resumen del mensaje.

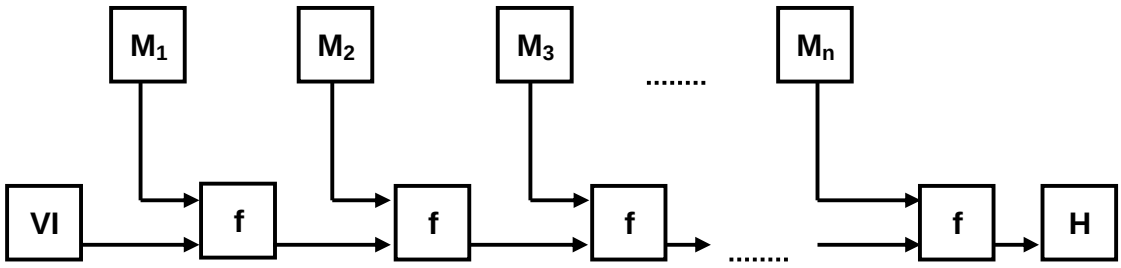


Figura N° 4.9 – Esquema de las Funciones de Resumen

El objetivo de estos algoritmos es que cada bit de salida dependa de todos los bits de entrada. Esto se consigue con diferentes iteraciones de operaciones que mezclan los bits entre ellos [5]**.**

Considerando las características que poseen los sistemas que se han analizado es importante introducir un margen de control de la integridad

que permita realizar el envío de información al momento de ser encriptada, es así como se debe asegurar que el mensaje recibido fue el enviado por la otra parte y no uno manipulado, para cumplir con este objetivo se utilizan funciones de dispersión unidireccional (Hash).

1.1.2 Sistemas de cifrado asimétrico

También son llamados sistemas de cifrado de clave pública. Este sistema de cifrado usa dos claves diferentes. Una es la clave pública y se puede enviar a cualquier persona y otra que se llama clave privada, que debe guardarse para que nadie tenga acceso a ella. Para enviar un mensaje, el remitente usa la clave pública del destinatario para cifrar el mensaje [5]**. Una vez que lo ha cifrado, solamente con la clave privada del destinatario se puede descifrar, ni siquiera el que ha cifrado el mensaje puede volver a descifrarlo. Por ello, se puede dar a conocer perfectamente la clave pública para que todo aquel que se quiera comunicar con el destinatario lo pueda hacer.**

Un sistema de cifrado de clave pública basado en la factorización de números primos se basa en que la clave pública contiene un número compuesto de dos números primos muy grandes. Para cifrar un mensaje, el algoritmo de cifrado usa ese compuesto para cifrar el mensaje. Para descifrar el mensaje, el algoritmo de descifrado requiere conocer los factores primos, y la clave privada tiene uno de esos factores, con lo que puede fácilmente descifrar el mensaje [31]**.**

En la figura N° 4.10 se aprecia la configuración de un sistema de asimétrico:

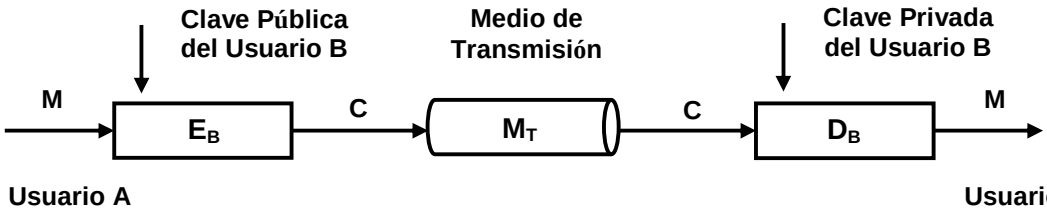


Figura N° 4.10 – Sistema de Cifrado Asimétrico

Hay que tener en cuenta que E_B y D_B son inversas dentro de un cuerpo, además se debe de tener en cuenta que se cifra con la clave pública del destinatario, de forma que conseguimos que solo él, al tener su clave privada pueda acceder al mensaje original.

En este segundo caso podemos observar como esta basado en el cifrado con la clave privada del emisor y al igual que antes hay que tener en cuenta que E_A y D_A son inversas dentro de un cuerpo.

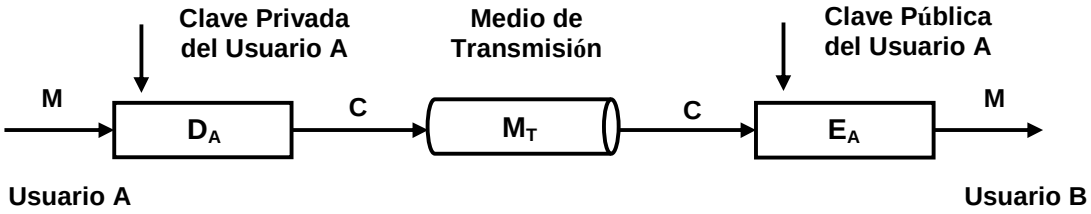


Figura N° 4.11 – Sistema de Cifrado Asimétrico

Es fácil, con los equipos de hoy en día, multiplicar dos números grandes para conseguir un número compuesto, pero es muy difícil la operación inversa.

Mientras que 128 bits se considera suficiente en las claves de cifrado simétrico, y dado que la tecnología de hoy en día se encuentra muy avanzada, se recomienda en este caso que la clave pública tenga un mínimo de 1024 bits. Para un ataque de fuerza bruta, por ejemplo, sobre una clave publica de 512 bits, se debe factorizar un numero compuesto de hasta 155 cifras decimales [5]**.**

1.1.2.1 *Uso de la criptografía de clave pública*

Hemos visto antes que las principales aplicaciones de la criptografía de clave pública son el intercambio de claves para proporcionar confidencialidad y la firma digital para proporcionar autenticidad y no repudio.

Un certificado de clave pública o certificado digital consta de tres partes básicas:

- **Una identificación de usuario como, por ejemplo, su nombre.**
- **El valor de la clave pública de este usuario.**
- **La firma de las dos partes anteriores.**

Si el autor de la firma es alguien en quien confiamos, el certificado sirve como garantía de que la clave pública pertenece al usuario que figura identificado en el certificado. Quien firma el certificado puede ser una autoridad que se responsabilice de verificar fehacientemente la autenticidad de las claves públicas. En este caso, se dice que el certificado ha sido generado por una autoridad de certificación (AC).

Puede haber distintos formatos de certificados, pero el más usado es el de los certificados X.509 (formato estándar para certificados de claves públicas, que incluye algoritmos de validación de la ruta de certificación).

1.1.2.2 *Cadenas de certificados y jerarquías de certificación*

Existe la posibilidad que una autoridad de certificación tenga un certificado que garantice la autenticidad de su clave pública, firmado por otra autoridad de certificación. Esta otra autoridad de certificación puede que si que la conozcamos, o puede que a su vez tenga un certificado firmado por una tercera autoridad de certificación, y así sucesivamente. De esta forma, se puede establecer una jerarquía de autoridades de certificación (AC) [5]**, donde la AC de nivel más bajo emite los certificados de usuario, y la AC de cada nivel son certificadas por una de nivel superior.**

Para poder verificar la autenticidad de la clave pública, un usuario puede enviar su certificado, más el certificado de la AC que lo ha emitido, más el de la AC que ha emitido este otro certificado, y así sucesivamente hasta llegar al certificado de una autoridad de certificación raíz. Esto es lo que se denomina una cadena de certificados (una condición que poseen estos certificados es la de auto firmarse). Un posible tipo de extensión de los certificados X.509 es basicConstraints, donde un campo de su valor indica si el certificado es de AC (se puede usar su clave para emitir otros certificados) o no. En el caso de que lo sea, otro subcampos permite indicar el número máximo de niveles de jerarquía que se sitúan por debajo de esta AC.

1.1.3 Sistemas de cifrado híbridos

Es el sistema de cifrado que usa tanto los sistemas de clave simétrica como el de clave asimétrica. Funciona mediante el cifrado de clave pública para compartir una clave para el cifrado simétrico. En cada mensaje, la clave simétrica utilizada es diferente por lo que si un atacante pudiera descubrir la clave simétrica, solo le valdría para ese mensaje y no para los restantes. En estos sistemas la clave simétrica es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un sólo paquete. El destinatario usa su clave privada para descifrar la clave simétrica y acto seguido usa la clave simétrica para descifrar el mensaje.

2 *SISTEMAS DE AUTENTICACION*

Uno de los servicios de seguridad que se requiere en muchas aplicaciones es el de la autenticación. Este servicio permite garantizar que nadie ha falsificado la comunicación.

Podemos distinguir dos tipos de autenticación:

2.1 Autenticación de mensaje

La autenticación de mensaje, también conocida como autenticación de origen de datos, permite confirmar que el origen *A* de un mensaje es auténtico, es decir, que el mensaje no ha sido generado por un tercero *C* que quiere hacer creer que lo ha generado *A*. Como efecto adicional, la autenticación de mensaje proporciona implícitamente el servicio de integridad de datos, que permite confirmar que nadie ha modificado un mensaje enviado por *A*.

Existen dos grupos de técnicas para proporcionar autenticación de mensaje, los cuales serán analizados a continuación:

2.1.1 *Códigos de autenticación de mensaje (MAC)*

Un código de autenticación de mensaje se obtiene con un algoritmo *a* que tiene dos entradas: un mensaje *M* de longitud arbitraria, y una clave secreta *k* compartida por el originador y el destinatario del mensaje [5]**.**

Un posible algoritmo MAC consiste en aplicar al mensaje *M* un cifrado en bloque en modo CBC con la clave *k*, y tomar el último bloque cifrado como código CMAC. Los algoritmos MAC usados actualmente, suelen estar basados en una función Hash. Por ejemplo, la técnica de calcular el resumen a partir de la unión del mensaje y la clave, o la de calcular el resumen del mensaje y cifrarlo con la clave, podrían servir como algoritmos MAC. Para mejorar la seguridad contra ciertos ataques, muchos protocolos usan una técnica de autenticación de mensajes un poco más sofisticada, conocida como HMAC.

2.1.2 *Firmas Digitales*

Los códigos MAC, dado que se basan en una clave secreta, sólo tienen significado para quienes conozcan dicha clave. Si *A* envía mensajes a

_B_ autenticados con una clave compartida, sólo _B_ podrá verificar la autenticidad de estos mensajes.

Si se presentase un conflicto en que _A_ denegase la autoría de un mensaje autenticado, _B_ no podría demostrar delante de un tercero imparcial (un árbitro) que el mensaje lo generó _A_. Revelar la clave secreta no sería prueba suficiente ya que, por el hecho de ser conocida por las dos partes, siempre habría la posibilidad que el mensaje en disputa y el código de autenticación los hubiera generado _B_.

En cambio, si _A_ autentica los mensajes adjuntándoles la firma digital calculada con su clave privada, todo el mundo podrá verificarlos con su clave pública.

Esta técnica de autenticación proporciona, como efecto adicional, el servicio de no repudio. Esto quiere decir que un destinatario _B_ puede demostrar fehacientemente ante un tercero que un mensaje ha sido generado por _A_ [5]**.**

2.2 Autenticación de Entidad

Este tipo de autenticación permite confirmar la identidad de un participante _A_ en una comunicación, es decir, que no se trata de un tercero _C_ que dice ser _A_.

De esta forma la autenticación de entidad se utiliza cuando en una comunicación una de las partes quiere asegurarse de la identidad de la otra. Normalmente, esta autenticación es un requisito para permitir el acceso a un recurso restringido. Por ejemplo, una cuenta de usuario en un equipo, dinero en efectivo en un cajero automático, acceso físico a un cuarto entre otros.

En general, las técnicas utilizadas para la identificación de un usuario _A_ pueden estar basadas en:

- **Algo que _A_ sabe, pudiendo ser una contraseña o una clave privada.**

- **Algo que *A* tiene, como una tarjeta con banda magnética o una tarjeta con chip.**

- **Algo que *A* es, alguna propiedad asociada de tipo biométrico.**

Una diferencia entre la autenticación de mensaje y la autenticación de entidad es que la primera puede ser intemporal (es posible verificar la autenticidad de un documento firmado, por ejemplo, diez años atrás) mientras que la segunda normalmente se realiza en tiempo real. Esto quiere decir que para la autenticación de entidad se puede llevar a cabo un protocolo interactivo, en el que ambas partes se intercambien mensajes hasta que la identidad en cuestión quede confirmada.

A continuación veremos dos grupos de técnicas que se pueden utilizar para la autenticación de entidad:

- **Las basadas en contraseñas, también llamadas técnicas de autenticación débil.**

- **Las basadas en protocolos de reto-respuesta (En Ingles Challenge-response), también llamadas técnicas de autenticación fuerte y las que serán analizadas en los siguientes ítemes.**

2.2.1 Contraseñas

La idea básica de la autenticación basada en contraseñas es que el usuario *A* manda su identidad (su identificador de usuario, su nombre de login, etc.) seguida de una contraseña secreta X*A* (una palabra o combinación de caracteres que el usuario pueda memorizar). El verificador *B* comprueba que la contraseña sea válida, y si lo es da por buena la identidad de *A* [9].

A continuación se analizara el tipo de método mas conocido en base a la autenticación basada en contraseñas:

2.2.1.1 *Protección de tarjetas usando PIN*

Este tipo de protección se utiliza típicamente bajo métodos de autenticación basados en dispositivos físicos, como las tarjetas bancarias o los módulos SIM (Subscriber Identity Module) de los teléfonos móviles. Estos dispositivos requieren que el usuario introduzca un PIN (Numero de Identificación Personal). Por motivos de conveniencia de los usuarios, este PIN es un número de longitud corta (por ejemplo de cuatro cifras). En este caso, para evitar los ataques de fuerza bruta, el dispositivo se bloquea al tercer intento equivocado.

La protección que proporciona el bloqueo puede ser un inconveniente para el usuario legítimo que no tiene ninguna culpa de que alguien haya intentando descubrir su contraseña. Para evitarle este inconveniente, una posibilidad es que cada usuario tenga asociada otra contraseña de desbloqueo, mucho más difícil de adivinar (por ejemplo, un PIN de ocho cifras para desbloquear el PIN de cuatro cifras).

Otra posibilidad consiste en permitir múltiples intentos de autenticación, pero en lugar de responder inmediatamente con un mensaje de contraseña incorrecta, demorar esta respuesta con un tiempo de retraso, que irá creciendo a medida que se vayan enviando más contraseñas erróneas por parte del mismo usuario. Esto ralentizaría tanto un ataque que lo haría inviable a partir de unos pocos intentos. Y cuando el usuario legítimo utilice su contraseña correcta, el tiempo de respuesta será el normal.

2.2.2 ***Protocolos de Reto-Respuesta***

El problema que tienen los esquemas de autenticación basados en contraseñas es que cada vez que se quiere realizar la autenticación se tiene

que enviar el mismo valor al verificador. Cualquier atacante que consiga interceptar este valor fijo podrá suplantar la identidad del usuario a quien corresponda la contraseña.

Hay otro grupo de mecanismos donde el valor que se envía para la autenticación no es fijo, sino que depende de otro, generado por el verificador. Este último valor se llama reto, y se debe enviar al usuario *A* como primer paso para su autenticación. De esta forma *A*, haciendo uso de una clave secreta, calcula una respuesta a partir de este reto, y lo envía al verificador *B*. Por este motivo, estos mecanismos de autenticación reciben el nombre de protocolos de Reto-Respuesta.

El algoritmo para calcular la respuesta debe garantizar que no se pueda obtener sin saber la clave secreta. Esto permite al verificador confirmar que la respuesta sólo ha podido enviarla *A*. Si se utiliza un reto distinto cada vez, un atacante no podrá sacar provecho de la información que descubra interceptando la comunicación.

Dependiendo del protocolo, el verificador puede generar los retos de diversas maneras:

Secuencialmente : En este caso el reto es simplemente un número que se va incrementando cada vez (lo más normal es incrementarlo de uno en uno), y que por tanto no se repetiré nunca.

Aleatoriamente : El reto puede ser generado con un algoritmo Pseudoaleatorio [5] **(algoritmo sin secuencia lógica), pero la propiedad que tiene en este caso es que no es predecible para los atacantes.**

Cronológicamente: El reto se obtiene a partir de la fecha y hora actuales (con la precisión que sea adecuada para el protocolo). Este tipo de reto también se llama marca de hora o Timestamp. El receptor puede utilizar la marca de hora para saber si se trata de una nueva autenticación o si

alguien quiere reutilizar los mensajes de otra autenticación para intentar un ataque de repetición.

La ventaja de los retos cronológicos es que, para obtenerlos, sólo es necesario un reloj, que seguramente estará disponible en cualquier sistema, mientras que con los secuenciales y los aleatorios es preciso mantener información de estado (el número de secuencia o la entrada para calcular el siguiente número Pseudoaleatorio) para evitar repeticiones. El inconveniente es que es precisa una cierta sincronía entre los relojes. Si se utilizan técnicas como un servidor de tiempo que da la hora actual, también es preciso verificar que la hora obtenida sea auténtica, es decir, que un atacante no nos está engañando haciéndonos creer que es la hora que le interesa.

2.2.2.1 *Dispositivos para el cálculo de las respuestas*

El cálculo de la respuesta se puede hacer con algún Software diseñado para tal efecto, o también se puede utilizar un dispositivo, parecido a una pequeña calculadora, que guarda la clave secreta. El usuario introduce el reto mediante el teclado de esta calculadora, y en la pantalla aparece la respuesta.

Alternativamente, si el reto es cronológico, el dispositivo no tiene teclado, sino que va mostrando por la pantalla las respuestas en función de la hora actual (por ejemplo, cada minuto), en sincronía aproximada con el reloj del verificador.

Para más seguridad, el dispositivo también puede estar protegido con un PIN.

2.2.2.2 *Protocolos de Reto-Respuesta con clave simétrica*

Si el protocolo de Reto-Respuesta se basa en una clave *kAB*** **compartida por *A* y *B*, existen distintas formas de obtener esta clave. Por**

ejemplo, la pueden haber acordado directamente *A* y *B* de forma segura, o bien la pueden solicitar a un servidor de claves centralizado.

2.2.2.3 *Autenticación con función unidireccional*

Los protocolos anteriores hacen uso de un algoritmo de cifrado simétrico, pero también es posible utilizar funciones unidireccionales con clave secreta como, por ejemplo, los algoritmos de MAC. Para la verificación, en lugar de descifrar es preciso comprobar que el MAC sea correcto y, por tanto, los valores necesarios para calcularlo se han de enviar en claro.

3 *PROTECCION A NIVEL DE RED*

La protección a nivel de red garantiza que los datos que se envíen a los protocolos de nivel superior, como TCP o UDP, se transmitirán protegidos. El inconveniente es que puede ser necesario adaptar la infraestructura de la red y, en particular los Encaminadores para que entiendan las extensiones que es preciso añadir al protocolo IP para proporcionar esta seguridad.

3.1 Arquitectura de protocolo de seguridad de Internet (IPsec)

Este protocolo añade servicios de seguridad al protocolo IP, que pueden ser usados por los protocolos de niveles superiores (TCP, UDP, ICMP, etc.) [6]**.**

IPsec se basa en el uso de una serie de protocolos seguros, de los cuales hay dos que proporcionan la mayor parte de los servicios y los cuales serán analizados a continuación:

Protocolo AH : (Authentication Header) ofrece el servicio de autenticación de origen de los datagramas IP (incluyendo la cabecera y los datos de los datagramas).

Protocolo ESP : (Encapsulating Security Payload) Se encarga de ofrecer el servicio de confidencialidad, el de autenticación de origen de los datos de los datagramas IP (sin incluir la cabecera), o los dos a la vez.

Opcionalmente, cada uno de estos dos protocolos también puede proporcionar otro servicio, el de protección contra repetición de datagramas.

Para la autenticación y la confidencialidad es necesario utilizar unas determinadas claves, correspondientes a los algoritmos criptográficos que se apliquen.

Los agentes que intervienen en la arquitectura IPSec son:

- **Los nodos extremos de la comunicación, es decir, el origen y el destino final de los datagramas.**

- **Los nodos intermedios que suporten IPsec, llamados pasarelas seguras, como por ejemplo los Encaminadores o Cortafuegos con IPsec.**

El tráfico IPsec también puede pasar por nodos intermedios que no soporten IPsec. Estos nodos son transparentes al protocolo porque para ellos los datagramas IPsec son como cualquier otro datagrama IP.

La relación que se establece entre dos nodos que se envían datagramas IPsec el uno al otro se llama asociación de seguridad (AS). Estos dos nodos pueden ser o no los extremos de la comunicación, es decir, el origen de los datagramas o su destino final. Por tanto, podemos distinguir dos tipos de AS:

AS extremo a extremo : Se establecen entre el nodo que origina los datagramas y el nodo al cual van destinados.

AS con una pasarela segura : Al menos uno de los nodos es una pasarela segura (también pueden serlo ambos). Por tanto, los datagramas vienen de otro nodo y/o van hacia otro nodo.

También se debe considerar que las AS son unidireccionales, es decir, si *A* envía datagramas IPsec a *B*, y *B* envía datagramas IPsec a *A*, tenemos dos AS, una en cada sentido.

Cuando se establece una AS entre dos nodos, se utiliza uno de los dos protocolos básicos IPsec (AH o ESP) [5]**. Si se quiere utilizar ambos a la vez, se deberá establecer dos AS, una para cada protocolo.**

De esta forma puede pasar que en una comunicación entre dos nodos extremos intervengan diversas AS, cada una con sus nodos de inicio y de final y con su protocolo.

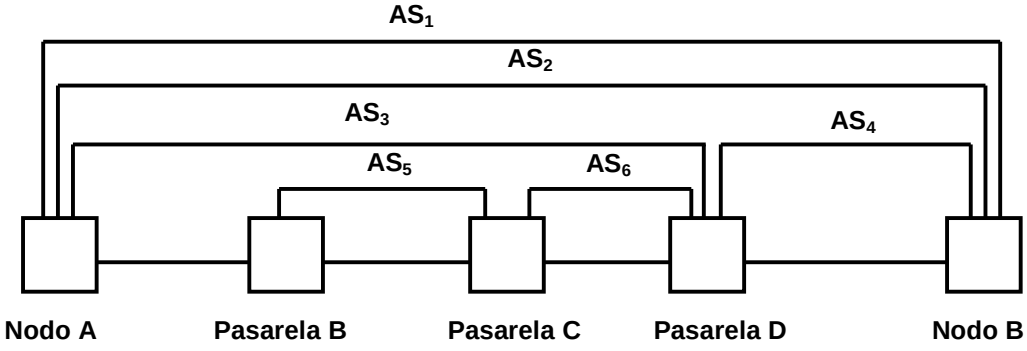


Figura N° 4.12 – Ejemplo de Combinación de Asociaciones de Seguridad

Cada nodo debe guardar información sobre sus AS, como por ejemplo los algoritmos criptográficos que utiliza cada una, las claves, etc. En la terminología IPsec, el lugar donde se guarda esta información se llama base de datos de asociaciones de seguridad (SAD). A cada AS le corresponden un número SAD llamado índice de parámetros de seguridad (SPI). Todas las AS que un nodo tenga establecidas con otro nodo han de tener SPI diferentes. Por lo tanto, cada AS en que participa un nodo queda identificado por la dirección IP de destino y su SPI.

Para cada datagrama que llega a un nodo IPsec, se consulta una base de datos de políticas de seguridad (SPD) donde se especifican criterios para determinar cual de las siguientes 3 acciones se debe realizar:

- **Aplicar servicios de seguridad IPsec al datagrama, es decir, procesarlo SPD según AH y/o ESP.**

- **Procesarlo como un datagrama IP normal, es decir, de forma transparente a IPsec.**

- **Descartar el datagrama.**

3.1.1 Protocolo AH

El protocolo AH define una cabecera que contiene la información necesaria para a la autenticación de origen de un datagrama.

Next Header	Payload Length	Reservado
Security Parameters Index (SPI)		
Numero de Secuencia		
Datos de Autenticación		

Figura N° 4.13 – Forma de la Cabecera AH

De acuerdo a la estructura de la cabecera AH es importante hacer una descripción de las partes que son incorporadas en la cabecera, las cuales son las siguientes:

Campo Next Header *: S*irve para indicar a que protocolo corresponden los datos que vienen a continuación de la cabecera AH.

Campo Payload Length : Indica la longitud de la cabecera (esta información se necesita porque el último campo es de longitud variable, ya que depende del algoritmo de autentificación).

Campo SPI : Sirve para identificar a que AS corresponde esta cabecera AH, y el número de secuencia que se utiliza si se quiere proporcionar el servicio de protección contra repetición de datagramas.

Campo de autentificación : Se establece mediante un código que se obtiene a partir del datagrama entero, según el algoritmo que corresponda a esta AS.

El nodo que reciba un datagrama con encabezamiento AH verificará el código de autentificación, y si es correcto dará el datagrama por bueno y lo procesará normalmente. Si a parte se utiliza el servicio de protección contra repeticiones, se necesita comprobar que el número de secuencia no sea repetido, si llegara ser a ser repetido descartará el datagrama.

3.1.2 Protocolo ESP

El protocolo ESP establece otro tipo de cabecera, con los mismos parámetros vistos anteriormente, pero distribuidos de diferente forma y en complemento con otros términos, en la figura N° 4.1 4 se puede ver la estructura de la cabecera ESP de un datagrama:

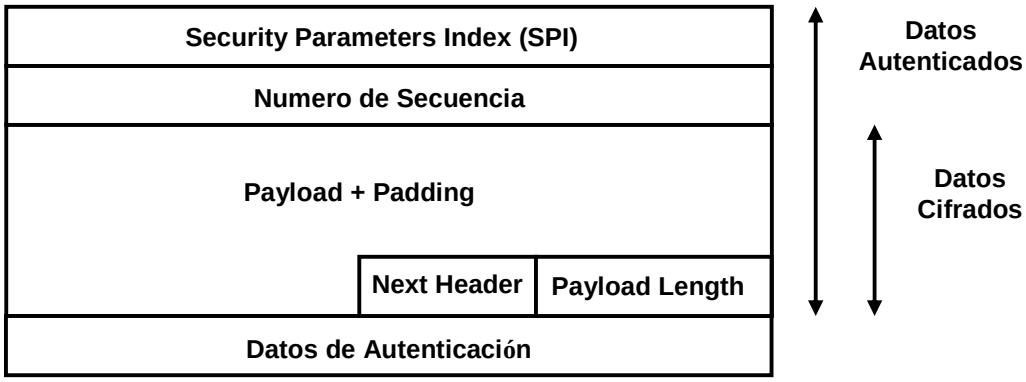


Figura N° 4.14 – Forma de la Cabecera ESP

Los campos SPI y número de secuencia son análogos a los de la cabecera AH. A continuación vienen los datos del datagrama (Payload), a los cuales puede ser necesario añadir bytes adicionales (Padding) si se utiliza un algoritmo de cifrado en bloque, para conseguir que el número de bytes a cifrar sea múltiple de la longitud de bloque. El campo Padding Length indica exactamente el número de bytes que se han añadido (puede ser 0). El campo Next Header indica de qué protocolo son los datos del datagrama.

Dependiendo del algoritmo de cifrado utilizado, puede ser necesario incluir antes de los datos cifrados parámetros como el vector de inicialización.

Dependiendo del servicio o servicios que proporcione esta cabecera ESP, puede ser que los datos estén cifrados (incluyendo el padding y los campos PaddingLength y Next Header), que se le añade un código de

autenticación calculado a partir de la cabecera ESP (pero no de las cabeceras que pueda haber antes), o ambas cosas a la vez.

El nodo que reciba un datagrama con cabecera ESP deberá verificar el código de autenticación, o descifrar los datos, o ambas cosas (por este orden, porque si se aplican los dos servicios primero se cifra y después se autentican los datos cifrados). Si a más se utiliza el servicio de protección contra repeticiones, también se debe comprobar el número de secuencia. Este último servicio, pero, sólo se puede utilizar cuando la cabecera ESP está autenticada.

3.2 Modos de uso de protocolo de seguridad de Internet (IPsec)

La arquitectura IPsec define dos modos de uso de los protocolos AH y ESP, dependiendo de como se incluyan las cabeceras correspondientes en un datagrama IP [32]**, estos modos son los siguientes:**

Modo transporte : La cabecera AH o ESP se incluye después de la cabecera IP convencional, como si fuera una cabecera de un protocolo de nivel superior, y a continuación van los datos del datagrama (por ejemplo, un segmento TCP con su cabecera correspondiente).

Modo túnel : El datagrama original se encapsula entero, con su cabecera y sus datos, dentro de otro datagrama. Este otro datagrama tendrá una cabecera IP en la cual las direcciones de origen y de destino serán las de los nodos inicio y final de la AS. De esta forma se dice que entre estos dos nodos hay un túnel dentro del cual viajan intactos los datagramas originales.

A continuación de la cabecera IP del datagrama externo (datagrama que vienes de la red externa) hay la cabecera AH o ESP.

Las siguientes figuras muestran la disposición de las cabeceras IPsec en cada modo. En estas figuras, trailer ESP se refiere a los campos Padding Length y Next Header de la cabecera ESP.

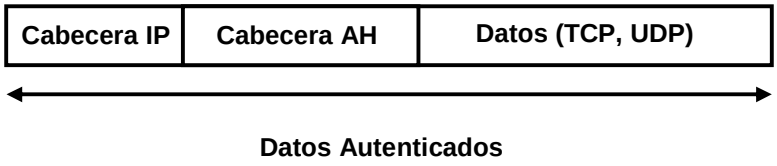


Figura N° 4.15 – Modo de Transporte AH

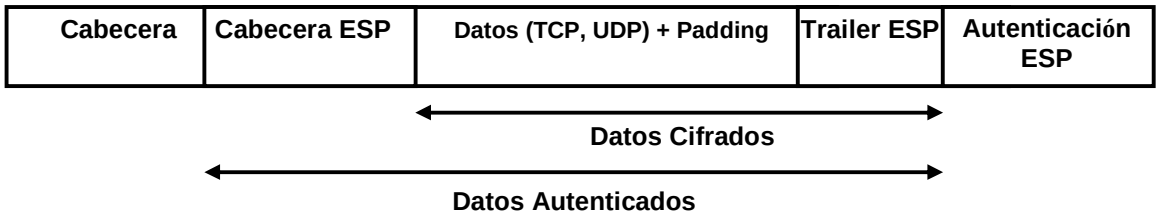


Figura N° 4.16 – Modo de Transporte ESP

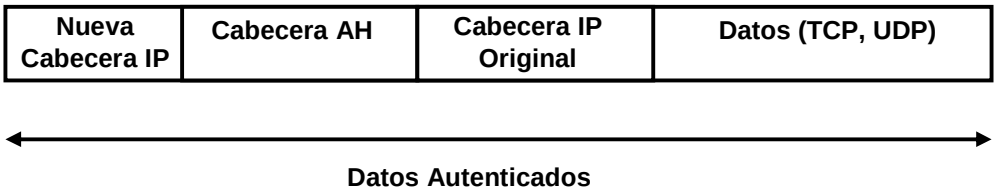


Figura N° 4.17 – Modo Túnel AH

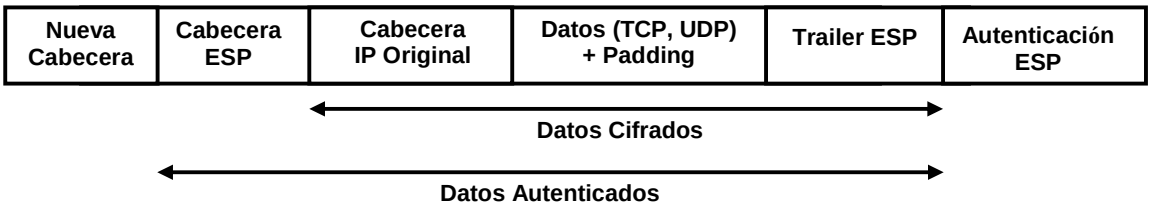


Figura N° 4.18 – Modo Túnel ESP

El protocolo IP antepone a que un datagrama se pueda fragmentar, y se puede dar el caso que los fragmentos de un mismo datagrama vayan por caminos diferentes hasta llegar a su destino final. Esto representaría un problema en una AS entre pasarelas seguras (o entre un nodo extremo y una pasarela segura) si se utilizara el modo transporte. Para evitar estas situaciones, en IPsec sólo se permite el modo transporte en las AS extremo a extremo.

El modo túnel no tiene este problema, aunque la AS sea entre pasarelas, cada datagrama tiene como dirección de destino la del nodo que hay al final del túnel, y todos los fragmentos finalmente tienen que llegar a este nodo. Por lo tanto el modo túnel se puede utilizar en cualquier AS, tanto si es extremo a extremo como si interviene una pasarela segura.

Puede haber diversas AS en el camino entre el originador de los datagramas y el destino final. Esto quiere decir que las disposiciones de cabecera AH y ESP que muestran las figuras anteriores se pueden combinar entre ellas. Por ejemplo, puede haber un túnel dentro de otro túnel, o un túnel dentro de una AS en modo transporte.

Otro caso que se puede dar es el de dos AS entre los mismos nodos de origen y de destino, una con el protocolo AH y la otra con el protocolo ESP. En este caso, el orden más lógico es aplicar primero ESP con servicio de confidencialidad y después AH, ya que de este modo la protección que ofrece AH se extiende a todo el datagrama resultante.

4 COMO PROTEGER LA CRIPTOGRAFÍA ASOCIADA A LA RED

En este punto se analizaran las principales formas de cómo proteger la criptografía que se vincula con la claves de acceso y verificación de información, como ha sido señalado anteriormente. De esta forma se pretende poner una barrera que permita dificultar el acceso a la claves.

A continuación se nombraran algunas formas de protección:

4.1 Reglas para evitar contraseñas fáciles

La solución de ocultar la lista de contraseñas codificadas da una seguridad parecida a la de la lista de contraseñas en claro. Si alguien descubre la lista (saltándose la protección contra lectura), puede realizar sin más problemas un ataque de diccionario.

Otro modo de dificultar este ataque es obligar a los usuarios a escoger contraseñas que cumplan unas determinadas reglas para que no sean fáciles de adivinar. Por ejemplo:

- **Que la contraseña tenga una longitud mínima.**
- **Que no sea todo letras ni todo números.**
- **Que las letras no coincidan con ninguna palabra de diccionario ni con combinaciones triviales de las palabras (como escribir las letras al revés entre otras condiciones).**
- **Que la contraseña no se derive del identificador del usuario, de su nombre, apellido.**

Con estas reglas se consigue que el espacio de contraseñas donde hacer la búsqueda sea más grande del que es habitual, y el ataque de diccionario necesite más tiempo.

4.2 Añadir complejidad a la codificación de las contraseñas

Otra solución para dificultar los ataques es ralentizarlos haciendo que cada contraseña cueste más de codificar. Por ejemplo, si el algoritmo de codificación no es directamente una función Hash sino un bucle de *N* llamadas a la función Hash, probar cada contraseña cuesta *N* veces más.

El valor *N* se puede escoger tan grande como se quiera, pero teniendo en cuenta que si es demasiado grande los usuarios legítimos también podrán notar que la autenticación normal es más lenta.

4.3 Uso de Frases de una mayor longitud

La propiedad que aprovechan los ataques de diccionario (consiste en intentar averiguar una contraseña probando todas las palabras del diccionario) es que el conjunto de contraseñas que utilizan normalmente los usuarios es un subconjunto muy pequeño de todo el espacio de contraseñas posibles.

Para ampliar este espacio se puede hacer que el usuario no utilice palabras relativamente cortas, de unos 8 caracteres, sino frases más largas, llamadas Passphrases. La codificación de estas Passphrases puede continuar siendo una función unidireccional, como por ejemplo una función Hash (con la misma longitud que en el caso de las contraseñas). La diferencia es que, si antes la lista de contraseñas codificadas contenía valores de entre un total de unos 150000 distintos, con Passphrases contendrá muchísimos más valores posibles, y la búsqueda exhaustiva del ataque de diccionario será mucho más larga.

5 *PROTECCIÓN DEL NIVEL DE TRANSPORTE SSL/TLS/WTLS*

Las protecciones a nivel de transporte están asociadas al uso de 3 protocolos de seguridad que permiten tener un resguardo en este nivel de modelo mediante el uso de sistemas criptográficos.

Los protocolos de seguridad son los siguientes:

Protocolo de transporte Secure Sockets Layer (SSL) : El protocolo SSL permite la autenticación de servidores, la codificación de datos y la integridad de los mensajes [26]**. Con SSL tanto en el cliente como en el servidor, sus comunicaciones en Internet serán transmitidas en formato codificado. De esta manera, puede confiar en que la información que envíe llegará de manera privada y no adulterada al servidor que usted especifique.**

Especificación Transport Layer Security (TLS) : Es un protocolo para el establecimiento de una conexión segura entre un cliente y un servidor. Mediante su uso se puede autenticar el cliente y el servidor y la creación de una conexión cifrada entre los dos.

Protocolo Wireless Transport Layer Security (WTLS) : Perteneciente a la familia de protocolos WAP (Wireless Application Protocol) para el acceso a la redes de dispositivos móviles. La mayoría de los protocolos WAP son adaptaciones de los ya existentes a las características de las comunicaciones inalámbricas, y en particular el WTLS está basado en el TLS.

5.1 Características del protocolo SSL/TLS

El objetivo inicial del diseño del protocolo SSL fue proteger las conexiones entre clientes y servidores Web con el protocolo HTTP. Esta

protección debía permitir al cliente asegurarse que se había conectado al servidor auténtico, y enviarle datos confidenciales, como por ejemplo un número de tarjeta de crédito, con la confianza que nadie más que el servidor sería capaz de ver estos datos.

Las funciones de seguridad no se implementaron directamente en el protocolo de aplicación HTTP, si no que se optó por introducirlas a nivel de transporte. De este modo podría haber muchas más aplicaciones que hicieran uso de esta funcionalidad.

Con este fin se desarrolló una interfaz de acceso a los servicios del nivel de transporte basada en la interfaz estándar de los Sockets (método para la comunicación entre un programa del cliente y un programa del servidor en una red).

En la figura se puede ver el diseño del protocolo SSL:

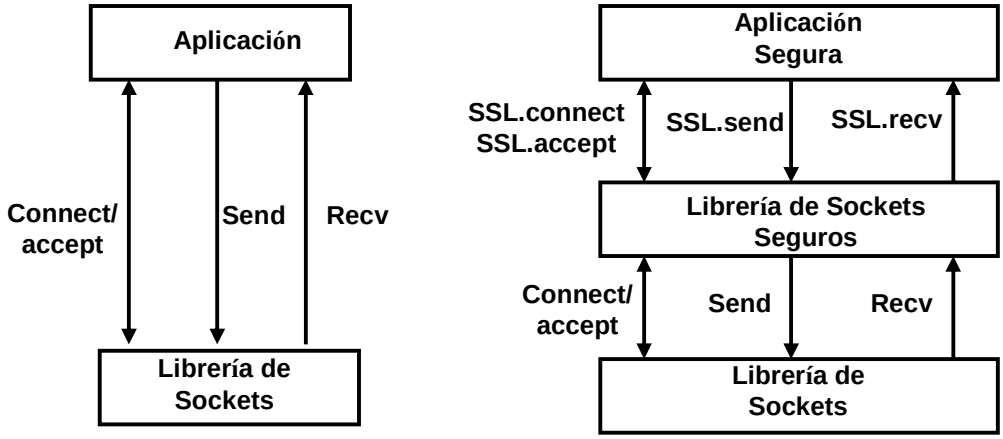


Figura N° 4.19 – Diseño de Protocolo SSL

Los servicios de seguridad que proporcionan los protocolos SSL/TLS son:

<u>Confidencialidad</u> : El flujo normal de información en una conexión SSL/TLS consiste en intercambiar paquetes con datos cifrados mediante claves simétricas (por motivos de eficiencia y rapidez). Al inicio de

cada sesión, cliente y servidor se ponen de acuerdo en que claves utilizarán para cifrar los datos.

Siempre se utilizan dos claves distintas, una para los paquetes enviados del cliente al servidor, y la otra para los paquetes enviados en sentido contrario. Para evitar que un intruso que esté escuchando el diálogo inicial pueda saber cuales son las claves acordadas, se sigue un mecanismo seguro de intercambio de claves, basado en criptografía de clave pública. El algoritmo concreto para este intercambio también se negocia durante el establecimiento de la conexión.

Autenticación de entidad : Con un protocolo de Reto-Respuesta basado en firmas digitales el cliente pude confirmar la identidad del servidor al cual se ha conectado. Para validar las firmas el cliente necesita conocer la clave pública del servidor, y esto normalmente se realiza a través de certificados digitales.

SSL/TLS también prevé la autenticación del cliente frente al servidor. Esta posibilidad, pero, no se usa tan a menudo porque muchas veces, en lugar de autenticar automáticamente el cliente a nivel de transporte, las mismas aplicaciones utilizan su propio método de autenticación.

Autenticación de mensaje : Cada paquete enviado en una conexión SSL/TLS, a más de ir cifrado, puede incorporar un código MAC para que el destinatario compruebe que nadie ha modificado el paquete. Las claves secretas par el cálculo de los códigos MAC (una para cada sentido) también se acuerdan de forma segura en el diálogo inicial.

A demás, los protocolos SSL/TLS están diseñados con estos criterios adicionales:

Eficiencia : Dos de las características de SSL/TLS, la definición de sesiones y la compresión de los datos, permiten mejorar la eficiencia de la comunicación.

Si el cliente pide dos o más conexiones simultáneas o muy seguidas, en lugar de repetir la autenticación y el intercambio de claves (operaciones computacionalmente costosas porque intervienen algoritmos de clave pública), hay la opción de reutilizar los parámetros previamente acordados. Si se hace uso de esta opción, se considera que la nueva conexión pertenece a la misma sesión que la anterior. En el establecimiento de cada conexión se especifica un identificador de sesión, que permite saber si la conexión empieza una sesión nueva o es continuación de otra.

SSL/TLS prevé la negociación de algoritmos de compresión para los datos intercambiados, para compensar el tráfico adicional que introduce la seguridad.

Extensibilidad : Al inicio de cada sesión, cliente y servidor negocian los algoritmos que utilizarán para el intercambio de claves, la autenticación y el cifrado (a más del algoritmo de compresión). Las especificaciones de los protocolos incluyen unas combinaciones predefinidas de algoritmos criptográficos, pero dejan abierta la posibilidad de añadir nuevos algoritmos si se descubren otros que sean más eficientes o más seguros.

5.2 Transporte seguro SSL/TLS

El transporte seguro que proporciona SSL/TLS puede ser establecida bajo dos Subcapas [33]**, las cuales son:**

Subcapa superior : Se encarga básicamente de negociar los parámetros de seguridad y de transferir los datos de la aplicación. Tanto los datos de negociación como los de aplicación se intercambian en mensajes.

<u>Subcapa inferior</u> : Estos mensajes son estructurados en registros a los cuales se les aplica, según corresponda, la compresión, la autenticación y el cifrado.

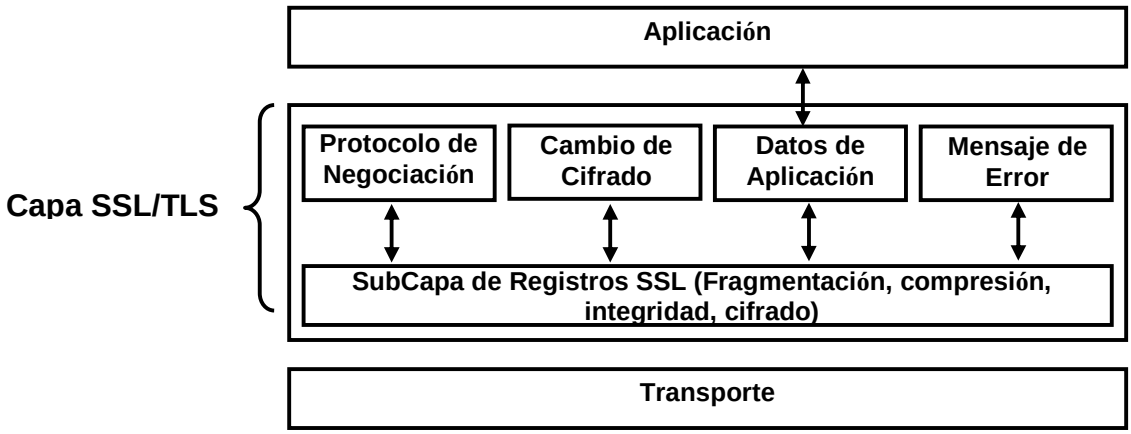


Figura N° 4.20 – Estructura de Capa SSL/TLS

El protocolo de registros SSL/TLS es el que permite que los datos protegidos sean convenientemente codificados por el emisor y interpretados por el receptor. Los parámetros necesarios para la protección, como pueden ser los algoritmos y las claves, se establecen de forma segura al inicio de la conexión mediante el protocolo de negociación SSL/TLS. A continuación veremos las características de cada uno de estos dos protocolos.

5.2.1 ***<u>Protocolo de Registros SSL/TLS</u>***

La información que se intercambian cliente y servidor en una conexión SSL/TLS se empaqueta en registros, los cuales tienen una configuración y formato como se aprecia en la figura N°4.21:

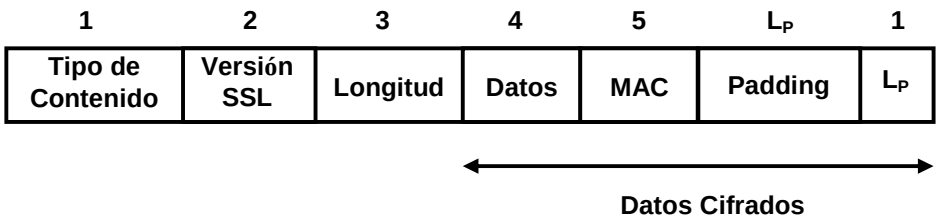


Figura N° 4.21- Formato de Registros SSL/TLS

El significado de cada campo es el siguiente:

El primer campo indica cual es el tipo de contenido de los datos, que puede ser:

- **Un mensaje del protocolo de negociación.**
- **Una notificación de cambio de cifrado.**
- **Un mensaje de error.**
- **Datos de aplicación.**

El segundo campo son dos bytes que indican la versión del protocolo.

El tercer campo indica la longitud del resto del registro. Por tanto, es igual a la suma de *Ld* y *LMAC* y, si los datos están cifrados con un algoritmo en bloque, *Lp*+1.

El cuarto campo son los datos, comprimidos si se ha acordado algún algoritmo de compresión.

El quinto campo es el código de autenticación (MAC). En el cálculo de este MAC intervienen la clave MAC, un número de secuencia implícito de 64

bits (que se incrementa en cada registro pero no se incluye en ningún campo) y, naturalmente, el contenido del registro.

La longitud de este campo depende del algoritmo de MAC que se haya acordado utilizar. Puede ser igual a 0 si se utiliza el algoritmo nulo, que es el que se utiliza al inicio de la negociación mientras no se ha acordado ningún otro.

El protocolo de registros SSL/TLS se encarga de formar cada registro con sus campos correspondientes, calcular el MAC, y cifrar los datos, el MAC y el Padding (Datos adicionales que puede ser necesario añadir a un texto en claro antes de aplicarle un algoritmo de cifrado en bloque, para que su longitud sea múltiple de la longitud del bloque) con los algoritmos.

En la fase de negociación, mientras no se hayan acordado los algoritmos, los registros no se cifran ni se autentican, es decir, se aplican algoritmos nulos.

5.2.2 *Protocolo de negociación SSL/TLS*

El protocolo de negociación SSL/TLS, también llamado protocolo de encajada de manos (Handshake Protocol), tiene por finalidad autenticar el cliente y/o el servidor, y acordar los algoritmos y claves que se utilizaran de forma segura, es decir, garantizando la confidencialidad y la integridad de la negociación [34]**.**

Como todos los mensajes SSL/TLS, los mensajes del protocolo de negociación se incluyen dentro del campo de datos de los registros SSL/TLS para ser transmitidos al destinatario. La estructura de un mensaje de negociación es la siguiente:

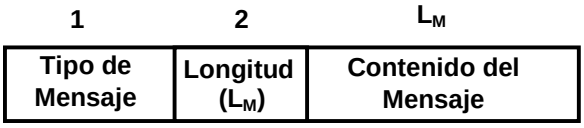


Figura N° 4.22 – Formato de Mensaje de Negociación SSL/TLS

El contenido del mensaje tendrá unos determinados campos dependiendo del tipo de mensaje de negociación del que se trate [34]**. En total hay 10 tipos distintos, que veremos a continuación en el orden en que se tienen que enviar:**

Petición de saludo (Hello Request) : Cuando se establece una conexión, el servidor normalmente espera que el cliente inicie la negociación. Alternativamente, puede optar por enviar un mensaje Hello Request para indicar al cliente que está preparado para empezar. Si durante la sesión el servidor quiere iniciar una renegociación, también lo puede indicar al cliente enviándole un mensaje de este tipo.

Saludo de cliente (Client Hello) : El cliente envía un mensaje Client Hello al inicio de la conexión o como respuesta a un Hello Request. Este mensaje contiene la siguiente información:

- **La versión del protocolo que el cliente quiere utilizar.**
- **Una cadena de 32 bytes aleatorios.**
- **Opcionalmente, el identificador de una sesión anterior, si el cliente desea volver a utilizar los parámetros que se han acordado.**
- **La lista de las combinaciones de algoritmos criptográficos que el cliente ofrece utilizar, por orden de preferencia. Cada combinación**

incluye el algoritmo de cifrado, el algoritmo de MAC y el método de intercambio de claves.

Saludo de servidor (Server Hello) : Como respuesta, el servidor envía un mensaje Server Hello, que contiene esta información:

- **La versión del protocolo que se usará en la conexión. La versión será igual a la que envió el cliente, o inferior si esta no es soportada por el servidor.**

- **Otra cadena de 32 bytes aleatorios.**

- **El identificador de la sesión actual. Si el cliente envió uno y el servidor quiere reprender la sesión correspondiente, debe responder con el mismo identificador. Si el servidor no quiere reemprender la sesión (o no puede porque ya no guarda la información necesaria), el identificador enviado será diferente. Opcionalmente, el servidor puede no enviar ningún identificador para indicar que la sesión actual nunca no podrá ser reemprendida.**

- **La combinación de algoritmos criptográficos escogida por el servidor de entre la lista de las enviadas por el cliente. Si se reemprende una sesión anterior, esta combinación debe ser la misma que se utilizó entonces.**

- **El algoritmo de compresión escogido por el servidor, o el que se utilizó en la sesión que se reemprende.**

Si se ha decidido continuar una sesión anterior, cliente y servidor ya pueden empezar a utilizar los algoritmos y claves previamente acordados y

se saltan los mensajes que vienen a continuación pasando directamente a los de finalización de la negociación (mensajes Finished).

Certificado de servidor (Certificate) : Si el servidor puede autenticarse frente al cliente, que es el caso más habitual, envía el mensaje Certificate. Este mensaje normalmente contendrá el certificado X.509 del servidor, o una cadena de certificados.

Si el servidor no tiene certificado, o se ha acordado un método de intercambio de claves que no precisa de él, debe mandar un mensaje Server KeyExchange, que contiene los parámetros necesarios para el método a seguir.

Petición de certificado (Certificate Request) : En caso que se deba realizar también la autenticación del cliente, el servidor le envía un mensaje Certificate Request. Este mensaje contiene una lista de los posibles tipos de certificado que el servidor puede admitir, por orden de preferencia, y una lista las autoridades de certificación que el servidor reconoce.

Servidor de saludo de servidor (Server Hello Done) : Para terminar esta primera fase del diálogo, el servidor envía un mensaje Server Hello Done.

Certificado de cliente (Certificate) : Una vez el servidor ha mandado sus mensajes iniciales, el cliente ya sabe como continuar el protocolo de negociación. En primer lugar, si el servidor le ha pedido un certificado y el cliente tiene alguno de las características solicitadas, lo envía en un mensaje Certificate.

Intercambio de claves de cliente (Client Key Exchange) : El cliente envía un mensaje Client Key Exchange, donde el contenido depende del método de intercambio de claves acordado. En caso de seguir el método

RSA, en este mensaje hay una cadena de 48 bytes que se usará como secreto Pre-Maestro, cifrada con la clave pública del servidor.

Entonces, cliente y servidor calculan el secreto maestro, que es otra cadena de 48 bytes. Para realizar esta cálculo, se aplican funciones Hash al secreto pre-maestro y a las cadenas aleatorias que se enviaron en los mensajes de saludo.

A partir del secreto maestro y las cadenas aleatorias, se obtienen:

- **Las dos claves para el cifrado simétrico de los datos (una para cada sentido: de cliente a servidor y de servidor a cliente).**

- **Las dos claves MAC (también una para cada sentido).**

- **Los dos vectores de inicialización para el cifrado, si se utiliza un algoritmo en bloque.**

Verificación de certificado (Certificate Verify) : Si el cliente ha mandado un certificado en respuesta a un mensaje Certificate Request, ya puede autenticarse demostrando que posee la clave privada correspondiente mediante un mensaje Certificate Verify. Este mensaje contiene una firma, generada con la clave privada del cliente, de una cadena de bytes obtenida a partir de la concatenación de todos los mensajes de negociación intercambiados hasta el momento, desde el Client Hello hasta el Client Key Exchange.

Finalización (Finished) : A partir de este punto ya se pueden utilizar los algoritmos criptográficos negociados. Cada parte manda a la otra una notificación de cambio de cifrado seguida de un mensaje Finished. La notificación de cambio de cifrado sirve para indicar que el siguiente mensaje será el primer enviado con los nuevos algoritmos y claves.

El mensaje Finished sigue inmediatamente la notificación de cambio de cifrado. Su contenido se obtiene aplicando funciones Hash al secreto maestro y a la concatenación de todos los mensajes de negociación intercambiados, des de el Client Hello hasta el anterior a este (incluyendo el mensaje Finished de la otra parte, si ya lo ha enviado). Normalmente será el cliente el primer en enviar el mensaje Finished, pero en el caso de reemprender una sesión anterior, será el servidor quien lo enviará primero, justo después del Server Hello.

El contenido del mensaje Finished sirve para verificar que la negociación se ha llevado a cabo correctamente. Este mensaje también permite autenticar el servidor frente al cliente, ya que el primer necesita su clave privada para descifrar el mensaje Client Key Exchange y obtener las claves que se usarán en la comunicación.

Una vez enviado el mensaje Finished, se da por acabada la negociación, y cliente y servidor pueden empezar a enviar los datos de aplicación utilizando los algoritmos y claves acordados.

Los siguientes diagramas resumen los mensajes intercambiados durante la fase de negociación SSL/TLS:

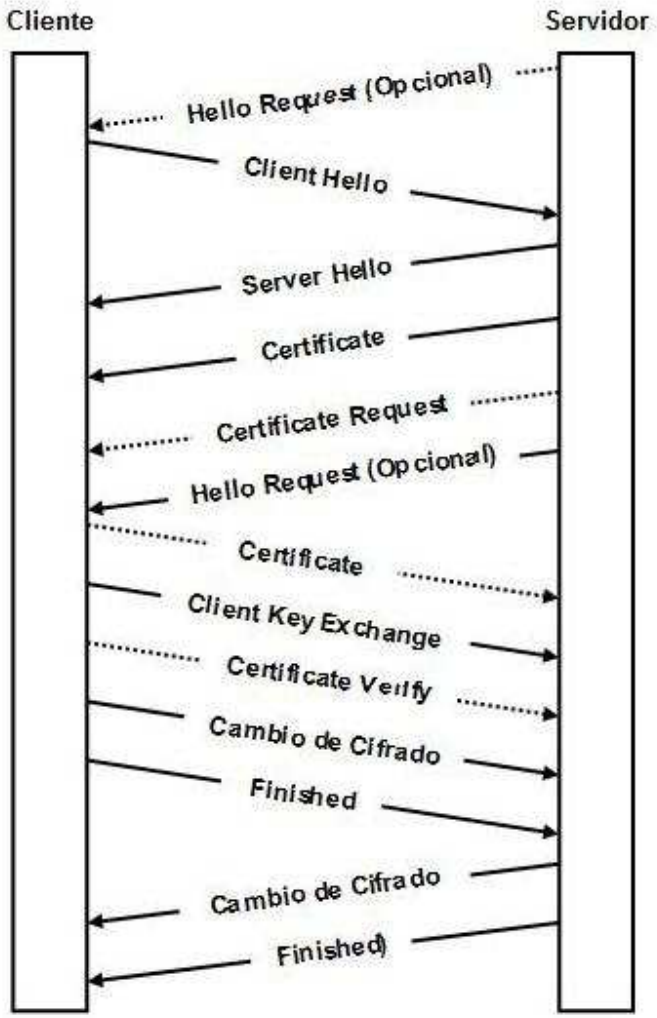


Figura N° 4.23 – Negociación de Sesión SSL/TLS

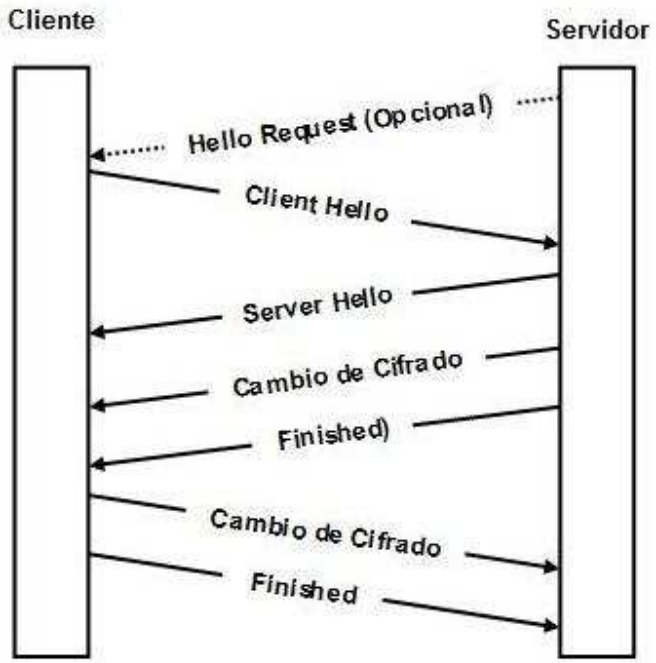


Figura N° 4.24 – Negociación de Sesión SSL/TLS Reemprendida

5.3 Ataques contra el protocolo SSL/TLS

Los protocolos SSL/TLS están diseñados para resistir los siguientes ataques:

5.3.1 *Lectura de los paquetes enviados por el Cliente y Servidor*

Cuando los datos se envían cifrados, un atacante que pueda leer los paquetes, por ejemplo utilizando técnicas de Sniffing, se enfrenta al problema de romper el cifrado si quiere interpretar su contenido. Las claves que se utilizan para el cifrado se intercambian con métodos de clave pública, que el atacante tendría que romper si quiere saber cuales son los valores acordados.

Es preciso advertir, pero, que dependiendo de la aplicación que lo utilice, el protocolo SSL/TLS puede ser objeto de ataques con texto en claro conocido. Por ejemplo, cuando se utiliza juntamente con HTTP para acceder a servidores Web con contenidos conocidos.

Si la comunicación es totalmente anónima, es decir sin autenticación de servidor ni cliente, existe la posibilidad de capturar las claves secretas. En esta captura el espía genera sus propias claves públicas y privadas, y cuando una parte envía a la otra información sobre su clave pública, tanto en un sentido como en el otro, el atacante la intercepta y la sustituye por la equivalente con la clave pública fraudulenta. Dado que el intercambio es anónimo, el receptor no tiene manera de saber si la clave pública que recibe es la del emisor auténtico o no.

En cambio, si se realiza la autenticación de servidor y/o cliente, es necesario enviar un certificado donde tiene que haber la clave pública del emisor firmada por una autoridad de certificación que el receptor reconozca, y por tanto no puede ser sustituida por otra.

5.3.2 *Suplantación de Servidor o Cliente*

Cuando se realiza la autenticación de servidor o cliente, el certificado digital debidamente firmado por la AC sirve para verificar la identidad de su propietario. Un atacante que quiera hacerse pasar por el servidor (o cliente) auténtico debería obtener su clave privada, o bien la de la AC que ha emitido el certificado para poder generar otro con una clave pública diferente y que parezca auténtico.

5.3.3 *Alteración de los paquetes*

Un atacante puede modificar los paquetes para que lleguen al destinatario con un contenido distinto del original (si están cifrados no podrá controlar cual será el contenido final descifrado, solamente sabrá que

será distinto al original). Si pasa esto, el receptor detectará que el paquete ha sido alterado porque el código de autenticación (MAC) casi con total seguridad será incorrecto.

Si la alteración se realiza en los mensajes de negociación cuando aun no se aplica ningún código MAC, con la finalidad por ejemplo de forzar la adopción de algoritmos criptográficos más débiles y vulnerables, esta manipulación será detectada en la verificación de los mensajes Finished.

5.4 Aplicaciones que utilizan SSL/TLS

Como hemos visto al inicio de este apartado, los protocolos SSL/TLS fueron diseñados para permitir la protección de cualquier aplicación basada en un protocolo de transporte como TCP.

La aplicación que utiliza esta característica es:

- **HTTPS (HTTP sobre SSL/TLS) es el protocolo más utilizado actualmente para la navegación Web segura.**

6 PROTECCIONES A NIVEL DE APLICACION

Las protecciones que existen a nivel de aplicación están dadas por los sistemas Cortafuegos que incorporan los sistemas operativos, por los Softwares Antivirus y Antispyware entre otros, pero a continuación se analizaran los tres nombrados anteriormente:

6.1 Sistema Cortafuegos incorporado en Sistema Operativo

Estos cortafuegos son un avanzado Softwares que actúa como un sistema de negación o aprobación de la ejecución de ciertas aplicaciones que son instaladas en el sistema operativo de un equipo, permitiendo restringir el acceso por parte de tercero a dicha aplicación y también

limitando el acceso de la aplicación a una red externa o la red global (Internet). De esta forma se esta favoreciendo el uso de la aplicación y del sistemas operativo en un equipo en particular, impidiendo el acceso a ejecuciones y uso de cualquier Software, ya tenga esta buena o malas intensiones.

Por ejemplo en la siguiente figura se puede apreciar la recomendación de activación del Cortafuegos que ofrece Windows:

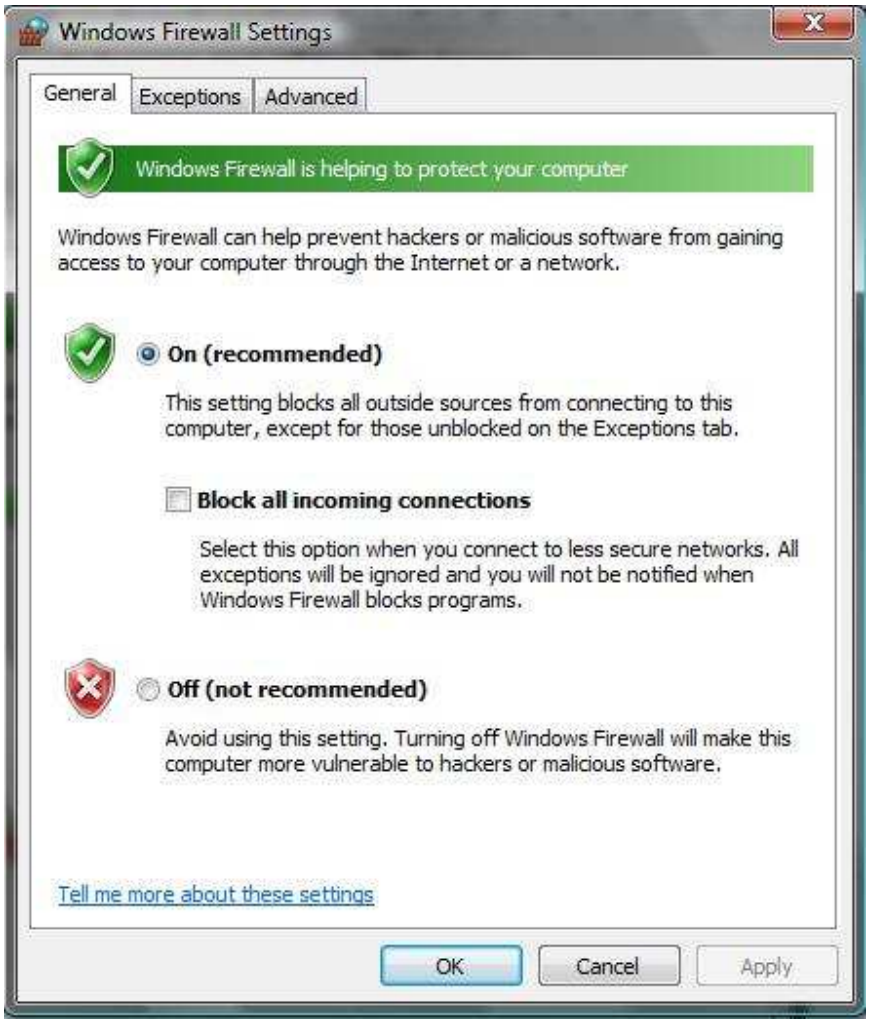


Figura N° 4.25 – Activación Cortafuegos de Windows

Y en la figura N° 4.26 se puede ver las excepciones de seguridad y ejecuciones de algunas de las aplicaciones que se encuentran en operación en el equipo.

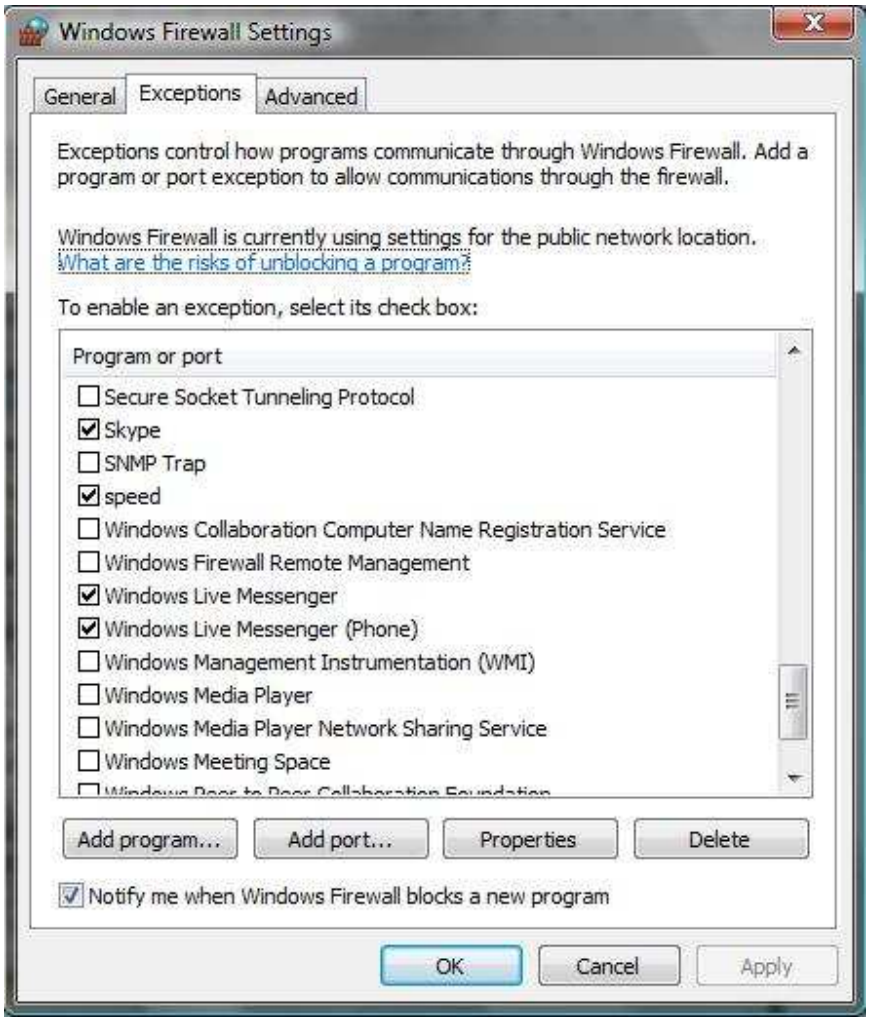


Figura N° 4.26 – Uso de aplicaciones con Excepción de Conexión

6.2 Softwares Antivirus

El Antivirus es un Software que impide el ingreso de Softwares maliciosos conocidos como virus, los cuales causan inconvenientes en el normal funcionamiento de un equipo, pudiendo estos ocasionar problemas en la ejecución de ciertas aplicaciones o impedir el normal funcionamiento del sistema operativo, eliminando archivos, suplantando o modificando archivos importantes. En si el virus es un código malicioso en un lenguaje determinado (lenguaje C, visual u/o lenguaje) que al ser ejecutado causa todos los inconvenientes nombrados anteriormente.

La ejecución de un virus puede estar dado por una serie de condiciones, que en algunos casos son imperceptibles por el usuario, copiando carpetas que contengan este código, al abrir un correo electrónico o descomprimir un archivo.

Es importante mencionar que lo que hace un antivirus es identificar alguno de los caracteres del código que se encuentran en la base de datos, entonces se tiene de esta forma un sistema de alerta respecto a todos los posibles códigos que presenten el mismo carácter.

Las consideraciones que se deben tener con los Antivirus son las constantes actualizaciones a las que deben estar sujetos y la configuración para tener una seguridad adecuada y un rendimiento optimo.

Los tipos de Antivirus existen en gran variedad, siendo catalogados comercialmente y gratis donde el usuario determinara cual es el más adecuado de acuerdo a sus requerimientos y el nivel de seguridad que desea.

7 REDES PRIVADAS VIRTUALES (VPN)

En este punto se analizara los mecanismos necesarios para establecer una red privada virtual (VPN) entre computador o entre redes de área local.

En este apartado veremos las características principales de las redes privadas virtuales [35]**.**

7.1 Definición y tipos de VPN

Una red privada virtual es una configuración que combina el uso de dos tipos de tecnologías:

- **Las tecnologías de seguridad que permiten la definición de una red privada, es decir, un medio de comunicación confidencial que no puede ser interceptado por usuarios ajenos a la red.**

- **Las tecnologías de encapsulamiento de protocolos que permiten que, en lugar de una conexión física dedicada para la red privada, se pueda utilizar una infraestructura de red pública, como Internet, para definir por encima de ella una red virtual.**

De esta forma una VPN es una red lógica o virtual creada sobre una infraestructura compartida, pero que proporciona los servicios de protección necesarios para una comunicación segura.

Dependiendo de la situación de los nodos que utilizan esta red, podemos considerar tres tipos de VPN [35]**:**

VPN entre redes locales : Es cuando en una institución dispone de redes locales en diferentes sedes, geográficamente separadas, en cada una de las cuales hay una red privada, de acceso restringido a sus empleados. Si interesa que desde una de sus sedes se pueda acceder a las

redes privadas de otras sedes, se puede usar una VPN para interconectar estas redes privadas y formar una red privada única.

VPN de acceso remoto : Cuando un usuario de una institución quiere acceder a la red privada desde un equipo remoto, puede establecer una VPN de este tipo entre este equipo y la red privada de la institución. El equipo remoto puede ser un computador que el usuario tiene en su casa, o un computador portátil desde el cual se conecta a la red de la institución cuando está de viaje.

VPN extranet : Es cuando a una institución le interesa compartir una parte de los recursos de su red privad con determinados usuarios externos, como por ejemplo proveedores o clientes. La red que permite estos accesos externos a una red privada se llama extranet, y su protección se consigue mediante una VPN extranet.

7.2 Configuraciones y Protocolos utilizados en VPN

A cada uno de los tipos de VPN que acabamos de ver le suele corresponder una configuración específica.

- **En las VPN entre Intranets (Redes Privada Internas) la situación más habitual es que en cada Intranet hay una pasarela VPN, que conecte la red local con Internet. Esta pasarela se comunica con la de las otras Intranets, aplicando el cifrado y las protecciones que sean necesarias a las comunicaciones de pasarela a pasarela a través de Internet. Cuando los paquetes llegan a la Intranet de destino, la pasarela correspondiente los descifra y los reenvía por la red local hasta el computador que los tenga que recibir. De esta manera es utiliza la infraestructura pública de Internet, en lugar de**

establecer líneas privadas dedicadas, que supondrían un coste más elevado.

También se aprovecha la fiabilidad y redundancia que proporciona Internet, ya que si una ruta no está disponible siempre se pueden encaminar los paquetes por otro camino, mientras que con una línea dedicada la redundancia supondría un coste aún más elevado.

- **En las VPN de acceso remoto, a veces llamadas VPDN, un usuario se puede comunicar con una intranet a través de un proveedor de acceso a Internet, utilizando tecnología convencional como por ejemplo a través de un módem ADSL. El ordenador del usuario ha de disponer de software cliente VPN para comunicarse con la pasarela VPN de la Intranet y llevar a cabo la autenticación necesaria, el cifrado, etc.**

  De este modo también se aprovecha la infraestructura de los proveedores de Internet para el acceso a la intranet, sin necesidad de llamadas a un módem de la empresa, que pueden llegar a tener un coste considerable.

- **El caso de las VPN extranet puede ser como el de las VPN entre intranets, en que la comunicación segura se establece entre pasarelas VPN, o bien como el de las VPN de acceso remoto, en que un cliente VPN se comunica con la pasarela de la intranet. La diferencia, pero, es que en este caso normalmente el control de acceso es más restrictivo para permitir solamente el acceso a los recursos autorizados.**

  La definición de una red virtual lleva a cabo mediante el establecimiento de túneles, que permiten encapsular paquetes de la red virtual, con sus protocolos, dentro de paquetes de otra red, que normalmente es Internet, con su protocolo, es decir IP.

Para la comunicación entre las distintas intranets, o entre el ordenador que accede remotamente y la intranet, se pueden utilizar los protocolos que sean más convenientes. Los paquetes de estos protocolos, para poderlos hacer llegar a su destino a través de Internet, se pueden encapsular en datagramas IP, que dentro suyo contendrán los paquetes originales. Cuando lleguen a su destino, se desencapsulan estos datagramas para recuperar los paquetes con el formato nativo del protocolo correspondiente.

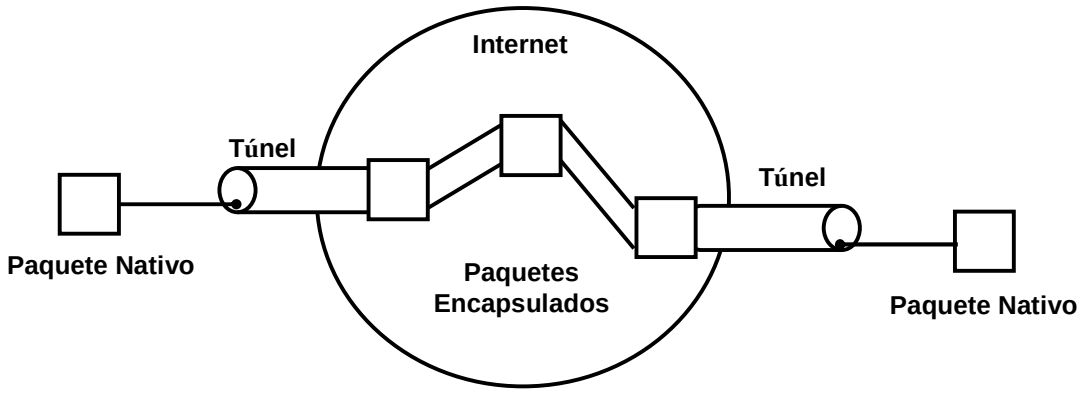


Figura N° 27 – Túneles de una VPN

Hay protocolos que pueden ser utilizados para establecer los túneles, dependiendo del nivel de la comunicación al cual se quiera realizar la protección.

<u>Túneles a nivel de Red</u> : El protocolo utilizado en la gran mayoría de configuraciones VPN es IPsec en modo túnel, generalmente con ESP par cifrar los datos, y opcionalmente con AH para autenticar los paquetes encapsulados. Las pasarelas VPN son, en este caso, pasarelas seguras IPsec.

<u>Túneles a nivel de Transporte</u> : El protocolo SSH (Secure Shell), ofrece la posibilidad de redirigir puertos TCP sobre un canal seguro, que

podemos considerar como un túnel a nivel de transporte (ver Capitulo 5, ítems 1.1). Des de este punto de vista, también se podría considerar una conexión SSL/TLS como un túnel a nivel de transporte que proporciona confidencialidad y autenticación. Habitualmente, este último tipo de túnel no sirve para cualquier tipo de tráfico si no solamente para datos TCP, y por tanto no se considera parte integrante de una VPN.

CAPITULO V:

Implementación de Protocolos y aplicaciones con un mayor nivel de Seguridad

1 IMPLEMENTACION DE PROTOCOLO DE SEGURIDAD SSH

El Protocolo SSH permite conectar de manera segura dos equipos a través de una red, ejecutar comandos de manera remota y mover datos entre los mismos. Proporciona autentificación fuerte, redirección de puertos TCP, sincronización de sistemas de datos, copias de seguridad, comunicaciones seguras sobre canales no seguros entre clientes/servidores y esta ubicado por debajo de la capa de transporte (Protocolo TCP) [25]**. Su seguridad reside en el uso de criptografía fuerte, de manera que toda la comunicación es encriptada y autentificada de forma transparente para el usuario.**

Es así como recoge los datos que el cliente quiere enviar y los reenvía por un canal seguro, donde al otro lado del canal se recogen los datos y se reenvían al servidor conveniente. En la figura N° 5.1 se puede ver un esquema general del uso de SSH:

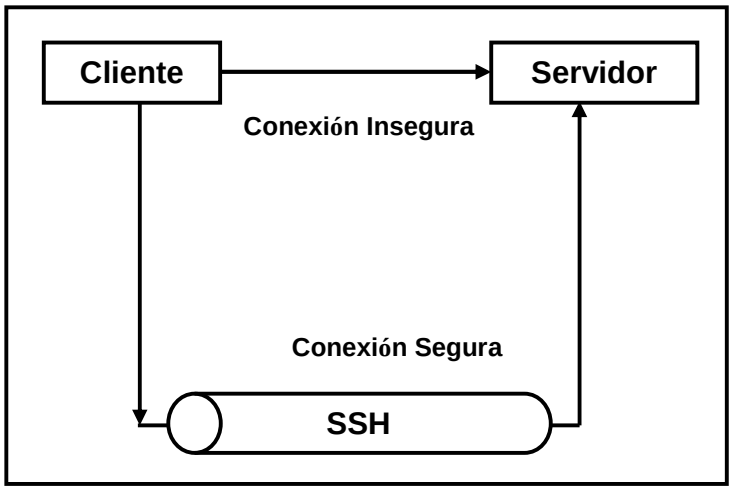


Figura N°5.1 – Implementación de Criptografía

El nombre de esta aplicación, SSH es la abreviatura de Secure Shell, que quiere decir versión segura del programa Remote Shell [8] **y mediante esta aplicación se impide:**

- **La intercepción de la comunicación entre dos sistemas donde un tercero en algún lugar de la red, puede entre entidades en comunicación hace una copia de la información que pasa entre ellas.**

- **La suplantación, cuando un equipo trata de hacerse pasar por otro equipo (un equipo confiable) y envía paquetes de datos procedentes del mismo.**

- **Enrutamiento de la IP de origen donde un equipo puede cambiar la IP de un paquete de datos procedente de otro, para que parezca que viene desde un equipo en el que se confía.**

- **Manipulación de los registros del servicio de nombres (DNS).**

- **Intercepción de contraseñas y datos a través de la red.**

Es importante mencionar que existen 2 versiones de este protocolo, las cuales son la versión SSH 1 y la versión SSH 2. Es así como SSH1 usa las claves del cliente y del servidor para autenticar, mientras que SSH2 solo usa las claves de la parte cliente [8]**.**

Como es obvio la versión número 2 es el replanteamiento de la versión 1, y se reestructura la versión de SSH y dando un nivel de seguridad aun mayor, ya que de esta forma se esta aumentando el nivel de encriptación, usando la versiones mas sofisticada de encriptación nombradas en el capitulo anterior (capitulo 4, ítems 1.1.1).

La entidad encargada de realizar estas modificaciones y el desarrollo comercialmente del protocolo SSH es SSH Communications Security. La cual establece las mejoras y las versiones de operación para los diferentes sistemas operativos.

1.1 Principales Características del Protocolo SSH

SSH proporciona servicios de seguridad equivalentes a los del protocolo SSL/TLS nombrados en el capitulo anterior, pero con ciertas características adicionales que los hacen mas seguro:

Confidencialidad : SSH sirve para comunicar datos, que habitualmente son la entrada de una aplicación remota y la salida que genera, o bien la información que se transmite por un puerto redirigido, y la confidencialidad de estos datos se garantiza mediante el cifrado.

SSH aplica un cifrado simétrico a los datos, por lo tanto, será necesario realizar previamente un intercambio seguro de claves entre cliente y servidor.

Un servicio adicional que proporciona SSH es la confidencialidad de la identidad del usuario. También permite ocultar ciertas características del tráfico de datos como, por ejemplo, la longitud real de los paquetes.

Autenticación de entidad : El protocolo SSH proporciona mecanismos para autenticar tanto el equipo servidor como el usuario que se quiere conectar.

La autenticación del servidor suele realizarse conjuntamente con el intercambio de claves.

Para autenticar al usuario existen distintos métodos, dependiendo de cuál se utilice, puede ser necesaria también la autenticación del ordenador cliente, mientras que otros métodos permiten que el usuario debidamente autenticado acceda al servidor desde cualquier ordenador cliente [25]**.**

Autenticación de mensaje : En SSH la autenticidad de los datos se garantiza añadiendo a cada paquete un código MAC calculado con una clave secreta. También existe la posibilidad de utilizar algoritmos MAC distintos en cada sentido de la comunicación.

SSH también está diseñado con los siguientes criterios adicionales:

Eficiencia : SSH contempla la compresión de los datos intercambiados para reducir la longitud de los paquetes, permitiendo negociar el algoritmo que se utilizará en cada sentido de la comunicación, aunque solamente existe uno definido en la especificación del protocolo.

EN SSH no está prevista la reutilización de claves de sesiones anteriores, ya que en cada nueva conexión se vuelven a calcular las claves.

Esto es así porque SSH está pensado para conexiones que tienen una duración larga, como suelen ser las sesiones de trabajo interactivas con un equipo remoto, y no para las conexiones cortas pero consecutivas, que son más típicas del protocolo de aplicación HTTP (que es el que inicialmente se quería proteger con SSL). De todas formas, SSH2 define mecanismos para intentar acortar el proceso de negociación.

Extensibilidad : En SSH se negocian los algoritmos de cifrado, de autenticación de usuario, de MAC, de compresión y de intercambio de claves.

Cada algoritmo se identifica con una cadena de caracteres que representa su nombre. Los nombres pueden corresponder a algoritmos oficialmente registrados, o bien a algoritmos propuestos experimentalmente o definidos localmente.

1.2 Capa de Transporte SSH

En la capa de transporte SSH se distinguen dos subniveles, donde el nivel superior está estructurado bajo tres protocolos, uno por encima del otro, y el nivel inferior que esta situado en el protocolo de paquetes SSH bajo tres protocolos que trabajan de forma simultanea [8] **como lo se puede ver en la figura N° 5.2:**

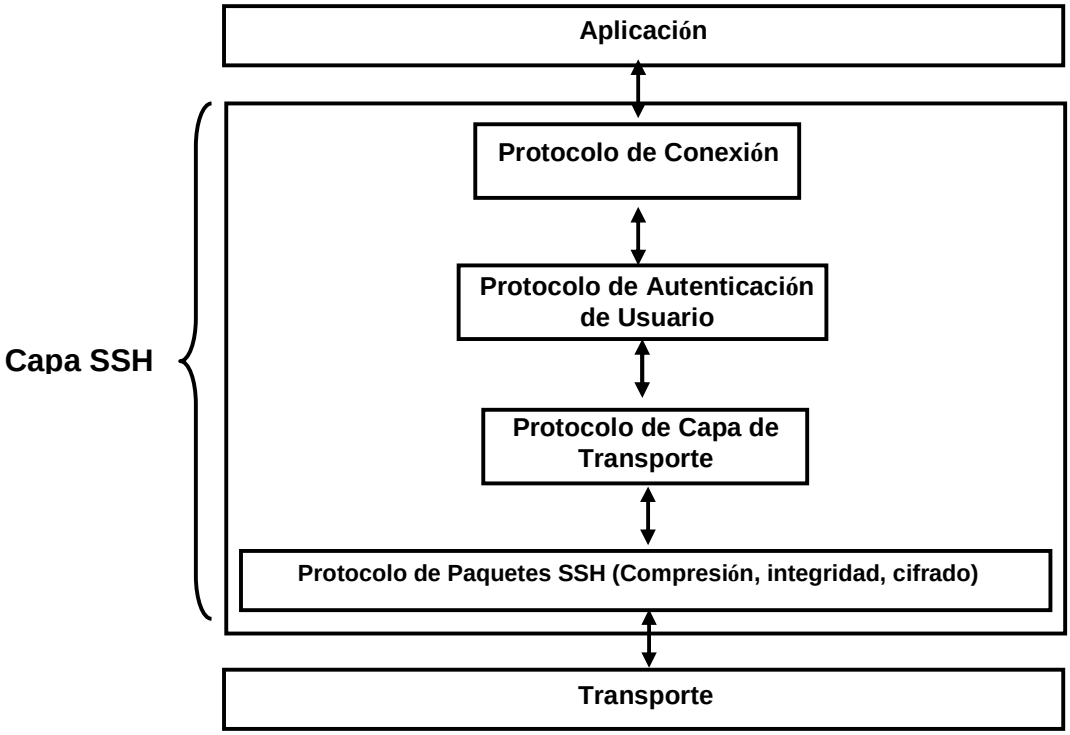


Figura N°5.2 – Estructura de la Capa de Transporte SSH

1.2.1 ***Protocolo de paquetes SSH***

El protocolo de paquetes SSH se encarga de construir e intercambiar las unidades del protocolo, que son los paquetes SSH.

En el momento de enviar datos, a los mensajes de los niveles superiores se les aplica la compresión, el código de autenticación MAC y el cifrado [8]**. En la recepción, a cada paquete se le aplica el procesamiento inverso (descifrado, verificación de autenticidad y descompresión).**

El formato de los paquetes SSH es el siguiente:

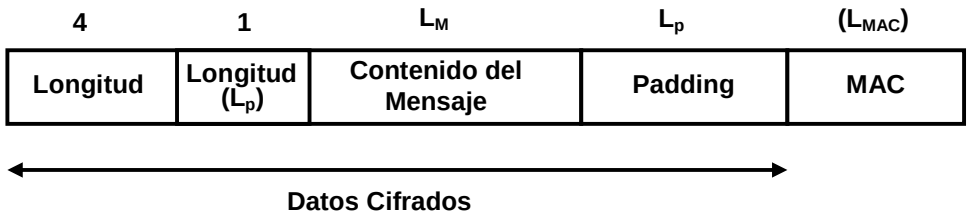


Figura N°5.3 – Formato de los paquetes SSH

Los campos existentes en un paquete SSH son los siguientes:

- **El primero es la longitud del resto del paquete, excluido el MAC (por lo tanto, es igual a 1+Lm+Lp).**

- **El segundo campo indica cuántos bytes de padding existen. Este número de bytes debe ser tal que la longitud total del paquete, excluido el MAC, sea múltiple de 8 (o de la longitud de bloque en los cifrados de bloque, si es más grande que 8).**

- **El tercer campo es el contenido del mensaje, comprimido si se da el caso.**

- **El primer byte del contenido siempre indica de qué tipo de mensaje se trata, y la estructura del resto de bytes depende del tipo.**

- **El cuarto campo son los bytes aleatorios de padding. Siempre están presentes, incluso cuando el cifrado utilizado sea en flujo, y su longitud tiene que ser como mínimo igual a 4. Por lo tanto, la longitud mínima de un paquete, sin contar el MAC, es de 16 bytes.**

- **El quinto campo es el código de autentificación MAC, obtenido mediante la técnica HMAC a partir de una clave secreta, un número de secuencia implícito de 32 bits y el valor de los otros cuatro campos del paquete. La longitud del MAC depende del algoritmo acordado, y puede ser 0 si se utiliza el algoritmo nulo.**

- **Cuando se cifran los paquetes, se aplica el cifrado a todos los campos excepto el del MAC, pero incluyendo la longitud. Eso significa que el receptor tiene que descifrar los 8 primeros bytes de cada paquete para conocer la longitud total de la parte cifrada.**

1.2.2 ***Protocolo de Capa de Transporte SSH***

El protocolo de capa de transporte se encarga del establecimiento de la conexión de transporte, de la autentificación del servidor y del intercambio de claves, y de las peticiones de servicio de los demás protocolos hacia el protocolo SSH.

Es así como el cliente se conecta al servidor mediante el protocolo TCP. El servidor debe estar escuchando peticiones de conexión en el puerto asignado al servicio SSH (puerto 22 estándar para protocolo TCP) que desea adquirir el cliente, para así establecer la conexión segura.

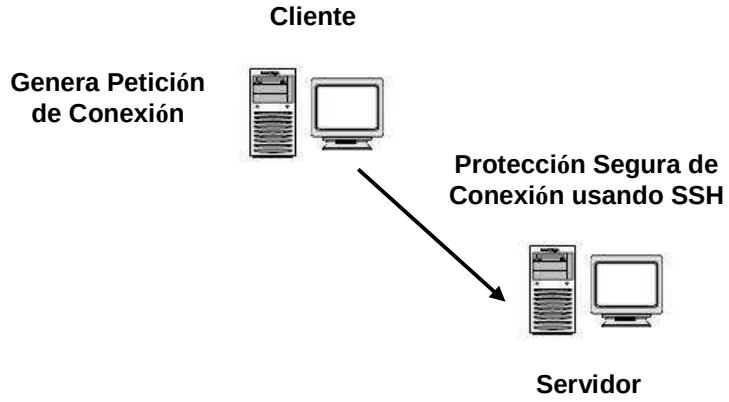


Figura N°5.4 – Conexión Segura usando SSH

Posterior a esta conexión el cliente y servidor pasan a intercambiar mensajes con el protocolo de paquetes SSH visto anteriormente, inicialmente sin cifrar y sin MAC.

Luego de esto se procede al intercambio de claves, donde cada parte envía un mensaje que contiene una cadena de 16 bytes aleatorios llamada Cookie (Fragmento de información), y las listas de algoritmos soportados por orden de preferencia, siendo primero los algoritmos de intercambio de claves (para cada sentido de la comunicación) y después los algoritmos de cifrado simétrico, de MAC y de compresión.

1.2.3 Protocolo de Autenticación de Usuario

En SSH se pueden ver diferentes tipos de autenticación de usuarios los que serán detallados a continuación:

Autenticación nula : El servidor permite que el usuario acceda directamente, sin ninguna comprobación, al servicio solicitado. Un ejemplo sería el acceso a un servicio anónimo.

Autenticación de listas de acceso : Es muy similar a la autenticación anterior, pero el servidor verifica que el sistema cliente sea efectivamente quien dice ser, para evitar los ataques de falsificación de dirección.

Autenticación basada en contraseña : El servidor permite el acceso si el usuario da una contraseña correcta.

Autenticación basada en clave pública : En lugar de dar una contraseña, el usuario se autentica demostrando que posee la clave privada correspondiente a una clave pública reconocida por el servidor.

1.2.4 ***Protocolo de conexión***

El protocolo de conexión gestiona las sesiones interactivas para la ejecución remota de comandos, mandando los datos de entrada de cliente a servidor y los de salida en sentido inverso. También se encarga de la redirección de puertos TCP [8]**.**

Como muestra la figura N° 5.5 con la redirección TC P es posible lograr que las conexiones que se realicen a un determinado puerto P_C del cliente, sean redirigidas a un puerto P_B de un equipo B desde el servidor, o que las conexiones que se realicen a un determinado puerto P_S del servidor sean redirigidas a un puerto P_D de un equipo D desde el cliente. De esta forma la conexión SSH se puede utilizar como túnel de otras conexiones a través de un Cortafuegos que esté situado entre el cliente y el servidor SSH.

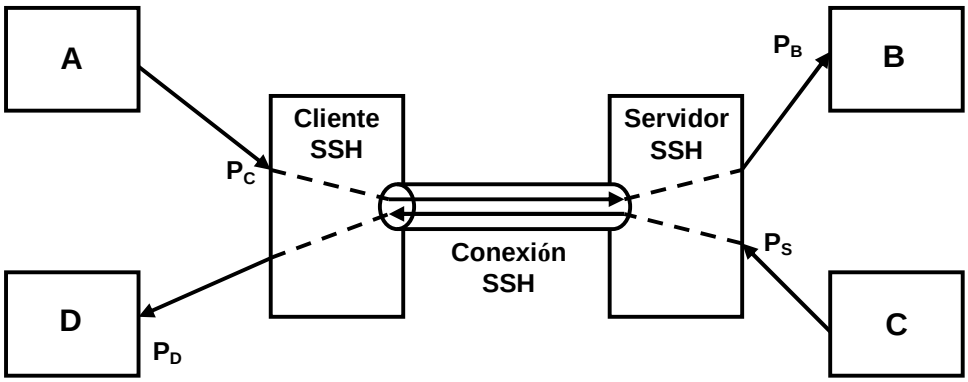


Figura N° 5.5 – Redireccionamiento de puerto TCP con SSH

Además SSH contempla la posibilidad de utilizar lo que se conoce como agente de autenticación el cual permite automatizar la autenticación del usuario basada en claves públicas cuando es necesario realizarla desde un equipo remoto.

Esto se puede ver en el ejemplo de la figura N°5. 6:

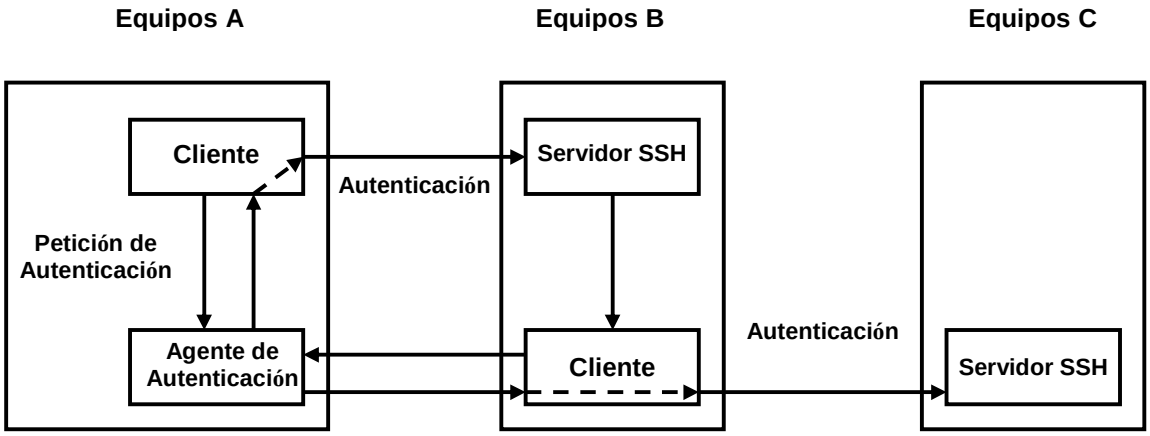


Figura N°5.6 – Uso del agente de Autenticación SSH

El usuario del equipo A utiliza un cliente SSH para conectarse al equipo B y trabajar con una sesión interactiva. El equipo A puede ser un equipo donde el usuario tenga guardada su clave privada. Entonces el usuario necesita establecer una conexión SSH desde el equipo B al equipo C y así poder autenticar con su clave personal.

El cliente del equipo B, en lugar de realizar directamente la autenticación, para lo que necesitaría la clave privada del usuario, pide al agente del equipo A que firme el mensaje adecuado para demostrar que posee la clave privada. Este esquema también se puede utilizar localmente por parte de los clientes del mismo equipo A.

Cada sesión, conexión TCP redirigida o conexión a un agente es un canal. Pueden existir distintos canales abiertos en una misma conexión SSH, cada uno identificado con un número en cada extremo (los números asignados a un canal en el cliente y en el servidor pueden ser diferentes).

2 IMPLEMENTACION INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

La tecnología PKI es la que se aplica a los sistemas de banca virtual en Internet garantizando la seguridad de las operaciones bancarias tradicionales con órdenes de compra/venda de valores, órdenes de transacciones interbancarias, gestión de cuentas, etc.

El establecimiento de una infraestructura de clave pública permite garantizar la confidencialidad cifrando los datos que viajarán por la red [6]**. Mediante el uso de firmas digitales, se garantiza la autenticidad, la integridad y el no repudio de los datos. Sin embargo, la estructura no se puede desplegar sin la existencia del servicio de los componentes necesarios que aporten la confianza en el uso de las claves públicas mediante la generación de los certificados, su gestión y revocación cuando sea necesario.**

Para el despliegue de la infraestructura se precisan los siguientes componentes:

Autoridad de Certificación (AC) : La AC emite certificados para las partes que intervienen y le da una valides a quien nos presenta una clave pública es quien dice ser. La AC también mantiene las listas de revocación de certificados para resolver los casos de robo, pérdida o suspensión de claves privadas. La seguridad de la AC es crítica, si se presenta un problema de seguridad que afecte a la AC puede afectar a toda la infraestructura existente.

Directorio : El directorio es la base de datos donde se publican los certificados. De esta forma, los certificados están disponibles todas las entidades. En el directorio, además se guardan otros datos las listas de revocación.

Actualización, históricos y copias de claves : Son los componentes que permiten la renovación del certificado, y el uso de claves antiguas. En los sistemas donde interviene datos cifrados hay que suministrar el servicio de recuperación de claves.

Soporte para el no repudio : La protección de las claves privadas puede ser crítica para el no repudio de las firmas digitales realizadas. Los sistemas basados en tarjetas criptográficas son los que ofrecen las mayores garantías. Estos componentes deben existir y pueden estar gestionados por la propia entidad bancaria, un consorcio u/o otra entidad externa.

La implantación de una solución de infraestructura de clave pública en una corporación tiene como finalidad dar la seguridad total de las comunicaciones, dando la mejor solución a los problemas de integridad, confidencialidad y acreditación. En una estructura PKI, los clientes en adelante usuarios y servidores disponen de un par de claves asimétricas, guardando la privada preferiblemente en una tarjeta inteligente y distribuyendo la pública en un certificado emitido por un centro certificador. La AC garantiza la autenticidad de los datos que figuran en el certificado (nombre, clave pública, etc.) durante un período de validez también indicado en el propio certificado, definido por la AC. El certificado también indica los usos de su clave privada.

Los problemas más inmediatos que soluciona una estructura PKI son:

Control de acceso : Acreditación de usuarios en servidores.

No repudio : La firma digital, que tiene asociadas las propiedades de autentificación e integridad, posibilita que el firmante no pueda repudiar su acción.

Confidencialidad : Cifrado de datos usando la clave pública de los destinatarios.

2.1 Características de la PKI

El sistema de Infraestructura de clave pública permite:

- **Establecer un servicio de acreditación fuerte para accesos a servicios. Los basados en Web son especialmente cómodos de implantar este sistema.**

- **Ofrecer la plataforma electrónica para que los usuarios puedan firmar digitalmente datos.**

- **Ofrecer la plataforma tecnológica para que los usuarios puedan ejecutar programas en su navegador de forma segura (firma de código).**

- **Ofrecer la plataforma para que los servidores puedan ser certificados y garantizar de esta forma su autenticidad.**

- **Total integración en cualquier solución futura basada el PKI (redes privadas virtuales, accesos a servidores, etc.).**

2.1.1 *Características de los Certificados emitidos*

Los certificados emitidos se deben ajustar a las especificaciones X509v3 (estándar de certificación) y soportar las extensiones de los exploradores. Esta característica permite la generación de certificados sin tener que conocer qué software va a usar el cliente, requisito importante en

entornos donde no existe una política clara de soporte a un único proveedor [6]**.**

Se generan diferentes tipos de certificados:

- **Certificados de cliente para acreditarse en servidores seguros y firmar datos.**

- **Certificados para servidores.**

- **Certificados para programadores que permiten firmar código ejecutable para garantizar a los usuarios la autenticidad del programa. Es la forma más segura de acabar con los virus.**

Es importante destacar que no se precisa de modo alguno de la clave de cifrado ya que las comunicaciones entre el cliente y la entidad se realiza sobre una conexión cifrada mediante el uso del protocolo SSL.

2.2 Modelos de firma y navegación

En los modelos de seguridad de PKI se distinguen tres modelos [13]**:**

Modelo de seguridad Web : Usa los mecanismos de seguridad de que disponen los navegadores más populares (Internet Explorer).

Modelo de seguridad Proxy : Donde se desconfía de la seguridad de los navegadores y se controla ésta mediante programas independientes (que interpretan la política de seguridad corporativa) [36]**.**

Modelo de seguridad mixto : Pretende suplir las carencias de seguridad de los exploradores añadiéndoles módulos o complementos (En Ingles Plug-ins).

El modelo de seguridad mixto permite garantizar el nivel máximo posible de seguridad en un entorno como el requerido, solucionando las carencias del modelo de seguridad Web, manteniendo el nivel óptimo de libertad de los usuarios en la elección de su plataforma de trabajo y evitando en la medida de lo posible los posteriores problemas de dimensionado de carga.

3 SEGURIDAD DE TRANSACCIONES ELECTRONICAS (SET)

SET (En Ingles Secure Electronic Transaction) es un protocolo que emula de forma electrónica, mediante el uso de certificados y firmas digitales, el pago de bienes y/o servicios mediante tarjeta de crédito [13]**.**

3.1 Arquitectura SET

Como método de pago basado en tarjeta, la solución SET conlleva la presencia de 3 nuevas entidades electrónicas a parte de los sistemas tradicionales ya utilizados en la actualidad. Los nuevos componentes son:

Entidad Comerciante SET : Es la entidad encargada de gestionar el pago del bien o servicio iniciado por un comprador. El pago siempre lleva asociado una transacción con un aceptador para la autorización del importe a pagar por el comprador. Habitualmente a esta entidad se le denomina POS (Point Of Sale) o TPV (Terminal Punto de Venta) virtual ya que su comportamiento, entre otras funciones, simula el de los sistema tradicionales.

Entidad Titular SET : Es la encargada de actuar en nombre del titular de la tarjeta virtual para realizar el pago. Habitualmente a esta entidad se le conoce como Cartera ya que su funcionalidad es muy similar a una cartera en la cual se almacenan las tarjetas.

Entidad Pasarela SET : Es encarga de hacer de puente entre el sistema aceptador SET y el sistema financiero propietario ya existente. Esta entidad es muy importante en cuanto supone la conexión de los sistemas y redes de autorización privados existentes con el mundo de Internet.

Esto se puede resumir en la figura N°5.7:

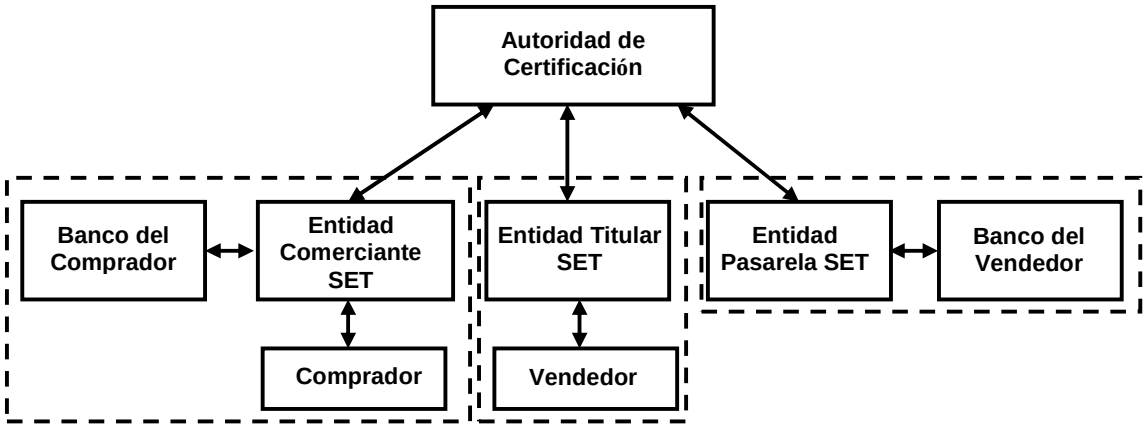


Figura N°5.7 – Componentes de SET

En el sistema SET la seguridad en las transacciones se ha cuidado hasta el último detalle. El sistema utiliza las últimas tecnologías de firma digital y certificación para llevar a cabo la protección de los datos a través de Internet.

Todas las entidades implicadas en el SET deben estar en posesión de un certificado válido para poder intervenir en una transacción de pago. Esto

quiere decir que tanto titulares, comerciantes y pasarelas SET deben de ser identificadas previamente y proveerles de un certificado para que puedan funcionar dentro del sistema.

Las entidades que generan los certificados para las entidades SET participantes se denominan AC SET o Autoridades de Certificación SET y generalmente son operadas por instituciones financieras capaces de emitir tarjetas (emisores) o instituciones asociadas, como bancos, que solicitan la emisión de tarjetas.

Las Autoridades de Certificación siempre están asociadas a una marca de tarjeta particular. Esto quiere decir que los certificados de todas las entidades sólo son válidos para una marca determinada siendo imposible utilizarlo en otro ámbito (Es imposible utilizar una tarjeta Visa como si se tratase de una MasterCard). De lo que se desprende que una entidad deberá estar en posesión de tantos certificados como marcas diferentes utilice (de ahí la acepción cartera para referirse a la entidad SET de titulares). Esto por otra parte hace muy flexible el sistema lo que, como se verá a continuación, nos permitirá utilizarlo dentro del ámbito de Marcas privadas.

Por último mencionar que existen varios tipos de Autoridades de Certificación SET dependiendo de su función y a quien certifiquen.

3.2 ***Protocolo de Pago SET***

El protocolo de pago SET define los mensajes e interacciones entre las entidades SET (comprador, comerciante y pasarela de pago) para llevar a cabo una transacción de pago desde que el comprador acepta pagar hasta que dicho pago se realiza mediante un abono en la cuenta del comerciante desde la cuenta del comprador [13]**.**

La siguiente figura muestra un esquema en el que aparecen los mensajes e interacciones típicas de un pago.

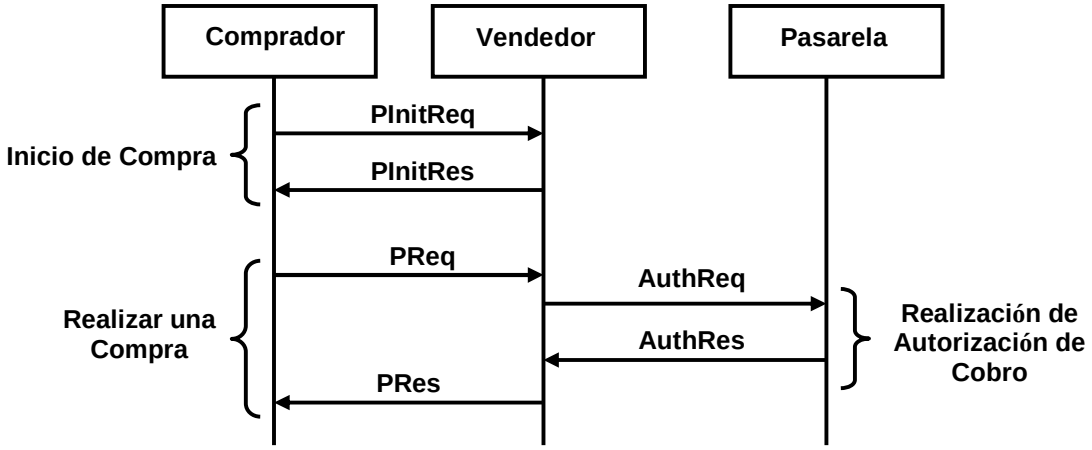


Figura N°5.8 – Protocolo de Pago SET

Como se observa existen 3 fases:

Fase de Inicialización : Corresponde al mensaje PInit y en la que el comprador contacta con el comerciante. El comprador informa de la marca de tarjeta que va a utilizar en el pago y el comerciante responde con un mensaje firmado que contiene el certificado de cifrado de la pasarela de pago asociada.

Fase de Pago : Corresponde al mensaje en que el comprador, si acepta el pago después de verificar la identidad del comerciante y las condiciones, realizara la orden de pago. La respuesta de este mensaje contiene información sobre la aceptación o denegación del pago proveniente de la autorización.

Fase de Autorización : Corresponde al mensaje Auth y en el que el comerciante solicita a la pasarela de pago (que a su vez solicitará al sistema financiero tradicional) si el comprador puede hacerse cargo de dicho pago (tiene crédito o saldo, la tarjeta no está revocada, etc.). La respuesta de este

mensaje contiene información sobre la aceptación o denegación del pago. En este esquema se ha optado realizar la captura o cobro del pago en la misma fase de autorización.

Mencionar que SET implementa el sistema de firma dual en el que el comprador en el mensaje PReq incluye datos protegidos para el comerciante y para la pasarela de forma que, el comerciante sólo puede ver los datos de la compra (pedido, modo de pago, cantidad, etc.) y la pasarela sólo puede ver los datos de pago (número de tarjeta, modo de pago, cantidad, etc.) que se enviarán en el mensaje AuthReq. De esta forma el comerciante nunca tendrá el número de tarjeta del comprador y la entidad financiera (a través de la pasarela) nunca tendrá los datos de la compra.

Como se puede observar del esquema presentado la fase de autorización ocurre durante la fase de pago. A esta modalidad se le conoce como pago en línea inmediato y es la más utilizada, aunque SET admite diferentes modalidades siendo un sistema que se adapta a los sistemas existentes en diferentes países. Además de las fases y mensajes vistos, SET proporciona también servicios para retrocesos o cambios de autorizaciones realizadas.

Es importante mencionar que tanto PKI como SET, son aplicaciones en base al uso del protocolo SSH, de los sistemas de cifrado y algoritmos de cifrado, certificados de autenticación, asociaciones de seguridad, contraseñas y protocolos SSL y TLS, nombrados en el capitulo 4. Estas 2 aplicaciones pasan por una restructuración de estas condiciones, para favorecer la seguridad de los sistemas bajo los que se implementa.

También se deben considerar las normas que se asocian a la seguridad de la información, siendo unas de las más reconocidas la generada por el estándar ISO, con su norma ISO 27001 en su versión BS 7799-2 (http://www.27001-online.com/index.htm), permitiendo algunas de las siguientes condiciones:

- **Constituye una especificación para establecer un Sistema de Administración de sistemas de información.**

- **Constituye el fundamento para procesos de certificación y auditoria de parte de terceros.**

- **Especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Administración.**

- **Establece los requerimientos para administrar la implementación de controles de seguridad.**

- **Está estructurado en cuatro etapas recurrentes (planificar, ejecutar, verificar y mejorar) para establecer un proceso de evolución y mejora continua.**

VI. Conclusiones

El desarrollo en las redes a permitido al modelo TCP/IP tener una mejora continua, considerando de manera significativa nuevos y más sofisticados sistemas de aplicación en la redes.

Debido a esto, la importancia que está adquiriendo conocer bien qué factores o condiciones pueden alterar el normal funcionamiento en el manejo de la información, es por eso que se debe tener en consideración los factores que perjudican la red y saber que resguardo tomar respecto a esas condiciones en particular.

Así es que se concluye esta investigación señalando:

- **La importancia que tiene la integración y manipulación de los sistemas a nivel de la capa de red, en donde los principales inconvenientes se presentan debido a la interceptación de información (ítem 2.2), la suplantación de mensajes y direcciones IP, los que se generan tras alterar el funcionamiento del Control de Acceso al Medio (ítem 2.2.1) y aprovechar las falencias físicas que presentan en la Tarjeta de Interfaz de Red, burlando la integridad, autenticidad y confidencialidad de los elementos y componentes de los equipos que sostienen y con los que se trabajan en la red.**

- **El manejo de los paquetes de datos a nivel de la capa de Internet, que al ser interceptados usando Software puede permitir manipularlos, ya sea modificando su contenido, adulterando su tamaño y extrayendo información que puede servir para un ataque mas profundo. Las falencias en este capa, se vinculan a las manipulaciones que pueden sufrir las verificaciones de conexión por parte del protocolo ICMP y de la fragmentación de datagramas IP.**

- **Las consideraciones que se deben tener respecto a la información vinculada a los puertos a nivel de la capa de Transporte que permiten realizar la identificación de conexiones validas por medio de sus protocolos y condiciones de sincronización, tanto del origen como en el destino por medio de numeraciones lógicas que se asignan a cada tipo de conexión, pudiendo realizar uso o no uso de los servicios que ofrece una conexión determinada. Donde las condiciones de uso se asocian a tres estados, los cuales son: abierto, cerrado y bloqueado. Las vulnerabilidades en la capa de transporte, están asociadas principalmente al manejo de herramientas y Software que se encuentran disponibles en la Red, que permiten examinar la disponibilidad de los puertos TCP y UDP y de manipular sus condiciones de conectividad.**

- **Los problemas mas considerables que se presentan en el modelo TCP/IP están presentes en la capa de Aplicación, la cual debido a la gran cantidad de información que se manipula y las falencias asociadas a la programación, permiten a terceras personas actuar de forma anónima, creando sofisticados Softwares maliciosos (Virus) para la manipulación de ciertos servicios. Estos pueden ocasionar la denegación de servicios importantes asociados a la conectividad mediante correos electrónicos, compra electrónica y servidores de nombres de dominios que soportan a determinados servicios que se encuentran en la red global.**

- **Debido a la gran cantidad de problemas encontrados, se hace indispensable la creación de herramientas, elementos y dispositivos que permiten resguardar la información, es por ello que en los capítulos numero III y IV. Es de esta forma que se comienzan a instaurar los primeros sistemas de seguridad a nivel de las diferentes capas del modelo TCP/IP.**

- **Los mecanismos de seguridad primarios se conocen como Cortafuegos, los cuales permiten realizar un filtro de la información en base a la configuración de equipos sofisticados (Encaminadores y pasarelas), de esta forma se puede tener un control en el flujo de la información y manejo de los paquetes de datos transferidos para optimizar el trabajo en la red. Estos sistemas de acuerdo a su arquitectura, pueden incorporar diferentes elementos que favorecerán la seguridad (DMZ y equipos Bastiones).**

  Es muy importante en la administración de los sistemas Cortafuegos, tener muy bien manejado el nivel de actualización y el mantenimiento, ya que así se puede anular en un alto porcentaje las vulnerabilidades que se presentan día a día.

- **En el análisis de los principales métodos de seguridad existentes se determinó que sumado a los sistemas Cortafuegos se tiene que considerar un resguardo mas personalizado de la información, es debido a ello que han sido desarrollados los sistemas criptográficos en base a los sistemas y algoritmos de cifrado que permiten codificar la información que se envía por la Red. Sumando a ello se debe considerar los sistemas de autenticación basados en el acceso mediante claves, protocolos seguros como SSL, TLS, asociaciones de seguridad, autoridades de certificación y redes privadas que permitirán restringir el acceso a una determinada red.**

- **Dentro de los protocolos que permiten tener aplicaciones seguras es el protocolo SSH, que brinda una respuesta mas fuerte y restringida a algunas de la vulnerabilidades del Modelo TCP/IP. Esto se debe principalmente, por la capacidad de alcance que tiene con su estructura de funcionamiento situada entre la capa de transporte y aplicación, haciendo hincapié en la integridad, el cifrado y la autenticación de la información que se manipula.**

Seguido al análisis del protocolo SSH, se detalló la principal aplicación segura utilizada por las instituciones bancarias a través de Internet, la cual se conoce como PKI, y que mediante los elementos de su infraestructura permite darle un importante resguardo a los datos y transacciones realizadas. También se detalló otra aplicación segura, asociada a la compra y venta de productos a través de Internet usando el Protocolo SET, que permite bajo su estructura manejar en detalle los niveles de seguridad asociados a la transacción.

- **Se debe considerar que la creación de más y mejores aplicaciones seguras y protocolos de seguridad se debe a la manipulación de los sistemas ya establecidos. Permitiendo en base a ellos las constantes mejoras y quizás nuevos incorporaciones que se encontraran en las redes.**

- **El análisis realizado está en base al modelo TCP/IP y a los sistemas operativos existentes. Es muy importante recalcar que los ataques de identificación de vulnerabilidad, ejecuciones u/o ordenes dadas, no pueden ser ejecutadas de la misma forma en los sistemas operativos (con las mismas instrucciones), sin embargo, existen complementos a éstas ejecuciones que hacen posible llegar al mismo fin, es decir, lograr la obtención de la información requerida.**

- **Debo señalar a modo personal que el trabajo realizado amplio considerablemente mis conocimientos en esta área de las comunicaciones que tan importante desarrollo tiene hoy en día. Considerando el auge que tiene el desarrollo de las comunicaciones y los futuros alcances en esta área, es que en mi desempeño laboral quiero enfocarme en el desarrollo de sistemas más seguros, ya sea en equipos móviles o portátiles (Celulares, Laptop, etc) que permitan tener una conectividad segura.**

VII. Referencia Bibliografíca

Textos

[1] **Gont F., Security Assessment of the Transmission Control Protocol (TCP), Centre for the protection of national infrastructure (CPNI), Usa 2008.**

[2] **Peguera M., Derecho y Nuevas tecnologías, Primera Edición, 2005**

[3] **Chris Hare, Internet Firewalls and Network Security, Vol 1, Second Edition 2004.**

[4] **Cheswick W.R., Firewalls and Internet Security, 5th Edition, 2001.**

[5] **Menezes J., Van Oorschot P.C., Handbook of Applied Cryptography, 5th Edition, 2001.**

[6] **Siles Raul, Análisis de la seguridad de la familia de protocolos TCP/IP y sus servicios asociados, Primera Edición, 2002.**

[7] **Oppliger, R. Security technologies for the Word Wide Web. First Edition, 2000.**

[8] **Garcia Leon N., Martinez U., Secure Shell, Primera Edición 2004**

[9] **Pk Yuen, Practical Cryptology and Web Security, 2006.**

Publicaciones

[10] **Martinez F.L., Sistemas distribuidos de Denegación de Servicio, 2000**

[11] **Elinos M.F., Perez J.A., Implementación de una DMZ, 2006 www.solusan.com/que-es-una-dmz.html**

[12] **Morales José, Cortafuegos, Comparativa entre las distintas generaciones y funcionalidades adicionales. Versión 1.1, 2002**

[13] **Buch Jordi, Jordan Francisco, Seguridad en la Transacciones en Internet, 2006.**

[14] **Paz Álvaro, Envenenamiento de Tablas Cache, 2007.**

Sitios Web

[15] **http://mervg.wordpress.com/2008/11/02/todo-sobre-redes**

[16] **http://es.kioskea.net/contents/attaques/attaque-syn.php3**

[17] **http://es.kioskea.net/contents/attaques/vol-session-hijacking.php3**

[18] **http://es.kioskea.net/contents/attaques/usurpation-ip-spoofing.php3**

[19] **http://es.kioskea.net/contents/attaques/attaque-teardrop.php3**

[20] **http://es.kioskea.net/contents/attaques/attaque-ping-de-la-mort.php3**

[21] **http://es.kioskea.net/contents/attaques/dos.php3**

[22] **http://es.kioskea.net/contents/attaques/passwd.php3**

[23] **http://debianitas.net/doc/minicomos/Utilizando%20Nmap/html/nmap-v1.html**

[24] **http://web.usal.es/~hernando/segi2009/3CifSim.pdf**

[25] **http://es.kioskea.net/contents/crypto/ssh.php3**

[26] **http://es.kioskea.net/contents/crypto/ssl.php3**

[27] **http://www.mundotech.net/comandos-ms-dos-para-trabajar-con-redes/**

[28] **http://www.elhacker.net/exploits/**

[29] **http://www.geocities.com/javierbri/c/cad.htm**

[30] **http://www.fing.edu.uy/inco/cursos/fsi/teorico/2009/FSI-2009-Criptografia.pdf**

[31] **http://www.wikilearning.com/curso_gratis/la_seguridad_en_informatica-introduccion_historica/3625-2**

[32] **http://www.dcc.uchile.cl/~cc51d/materia/ipsec/ipsec.pdf**

[33] **http://www.moratalaz.jazztel.es/pdfs/ssl.pdf**

[34] **http://leibniz.iimas.unam.mx/~yann/Crypto/Clase08.pdf**

[35] **http://www.potaroo.net/papers/1998-3-vpn/vpn.pdf**

[36] **http://computer.howstuffworks.com/firewall.html**

VIII. Glosario

AC : Autoridad de Certificación.

Agente de autenticación : Método que permite utilizar un servicio para mantener todas las claves privadas, y autenticar al usuario de forma centralizada.

AS : Asociación de seguridad.

Atacante : Persona que desea obtener información para visualizar, investigar y analizar. Y posteriormente en base al análisis realizar un ataque o contribución al sistema.

Autenticidad : Se refiere a estar seguros de la identidad de las personas y de los mensajes enviados, es decir la veracidad de los contenidos y personas que manipulan los contenidos.

Bastión : Es un equipo ubicado entre dos interfaces de redes que mantiene aislada la red local de la red externa.

Bibliotecas de vínculos dinámicos (DLL) : Son archivos que contienen funciones que se pueden llamar desde aplicaciones, permite de esta forma aislar las diferentes tareas, siendo el complemento de la ejecución en si.

Bucle : Es un tipo de estructura de control que permite repetir una o más sentencias múltiples en un código de programación.

Buffer Overflow : Defectos que se pueden presentar en un programa.

Cabecera : Forma parte de un paquete de datos y permite realizar una validación y control de los paquetes enviados a través de la red.

Campo TTL : Permite determinar el tiempo en la transmisión de los paquetes de datos, encargando de los limitarlos a un tiempo determinado si es necesario.

Cifrado : Es una condición que se le da a la información que circula por la red en base a algoritmos.

CMAC : Código de autenticación de mensajes en base a algoritmos.

Condición de promiscuidad : Es la desactivación de los filtros que posee la MAC.

Conexiones virtuales : Es un proceso que se realiza por medio de programas y la tarjeta de red para la transmisión de datos. Se realiza una serie de negociaciones o intercambio de tramas los cuales hacen posible un circuito virtual que permite el intercambio de información.

Contraseñas en claro : Son contraseñas cifradas en base a un texto en clave.

Cookie : Es un fragmento de información.

Datagramas : Son paquetes de datos.

Dirección de retorno : Dato almacenado dentro de la pila, que indica al programa en qué línea situarse luego de finalizar una función.

DES : Data Encryption Standard.

DMZ : Es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. Con ello permite brindar un nivel mas amplio de seguridad.

Encaminadores (Routers) : Permite realizar un direccionamiento y filtrado de los datos que circulan por la Red.

Envenenamiento de tablas caché : Método que permite realizar adulteración en la MAC.

Finger : Herramienta que permite identificar el número de usuarios y el nombre de ellos.

Fingerprinting : Es el proceso de búsqueda de huellas identificativas.

Firma digital : Es un método que usa criptografía asimétrica y permite autenticar una entidad (persona o servidor), y que tiene una función igual que la firma convencional.

Funciones Hash : Método para generar claves y funciones para resumir o identificar en base a probabilidades un gran conjunto de información.

Huellas Identificativas : Rastros de información que circula por la red o rastros que han quedado por el movimiento de la información.

IDEA : International Data Encryption Algorithm.

Indicadores espaciales (Flags) : Elemento del protocolo TCP que utiliza 6 bits para activar o desactivar el inicio de sesión en los puertos TCP.

Mas Fragmentos, MF : Es un indicar que permite verificar la existencia de mas fragmentos en un determinado paquete.

Multiplexión : División de los datos en unidades de datos más pequeñas para favorecer la velocidad en la trasmisión.

Paquetes : Es un conjunto de datos que se transmiten por una red.

Pasarela (Gateway) : Dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes y cuyo fin es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

Pila : Lista estructurada de datos que almacena y recupera datos.

Política por defecto : Es la condición que adquiere un equipo de acuerdo a su configuración, de aceptar ciertas condiciones o negarlas.

Predicción de secuencia TCP : Método que simulación la participación en una red, permitiendo tener acceso a una red en particular y lograr robar una sesión TCP.

Proxy : Es un programa o dispositivo que realiza una tarea de acceso a Internet en lugar de otro equipo. Es un punto intermedio entre un computador conectado a Internet y el servidor que está accediendo.

Pseudoaleatorio : Es un algoritmo de cifrado sin secuencia lógica.

Red Externa : Es la Red global de computadoras.

Red Interna : Es una red en particular de una organización que es separa de la Red global, pasando a ser una Red de carácter más privada.

Registros de auditorías : Conjunto de descripciones y datos de los mensajes de forma detallada.

Requests for Comments (RFC) : Interpretación de documentos técnicos y notas que circulan por la red.

RSA : Rivest, Shamir, Adelman, Iniciales Creadores.

SAD : Base de datos de asociaciones de seguridad.

Segmentos : Son Mensajes en diferentes tamaños.

Shellcode : Código arbitrario de carácter malicioso que permite la ejecución de comandos de sistema o modificaciones de las bibliotecas de vínculos dinámicos.

Sniffing : Proceso de recolección de información mediante Software.

Sniffers : Proceso de interceptación de información en la red que puede permitir posteriormente mediante el uso de Software realizar la captura, análisis e interpretación de datagramas que circulan por una red.

SPD : Base de datos de políticas de seguridad.

SPI : Índice de parámetros de seguridad.

SSH : Secure Shell Code.

Texto en claro : Información cifrada que es de carácter ininteligible.

Translación de Direcciones de Red (NAT) : Mecanismo que permite intercambiar paquetes de datos entre dos redes que se asignan mutuamente direcciones incompatibles.