UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

MONITOREO E IDENTIFICACION DE ATAQUES A REDES

Previa la obtención del Título de

INGENIERO EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL

ELABORADO POR:

DANIELA ESTEFANIA MUÑOZ CEDEÑO

DIRIGIDO POR:

ING. LUIS CÓRDOVA RIVADENEIRA, MSc.

GUAYAQUIL, ABRIL DE 2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por la estudiante DANIELA ESTEFANIA MUÑOZ CEDEÑO como requerimiento parcial para la obtención del título de INGENIERA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL.

DIRECTOR DE TESIS

_____

Ing. Luis Córdova Rivadeneira, MSc.

REVISOR

_____

Ing. Marcos Montenegro Tamayo, Mgs.

DIRECTOR DE LA CARRERA

_____

Ing. Miguel Armando Heras Sánchez

REVISOR

_____

Ing. Juan Carlos López Cañarte

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

INGENIERÍA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL

DECLARACIÓN DE RESPONSABILIDAD

DANIELA ESTEFANIA MUÑOZ CEDEÑO

DECLARO QUE:

El trabajo de titulación denominado "MONITOREO E IDENTIFICACION DE ATAQUES A REDES", ha sido desarrollado con base a una investigación íntegra, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del trabajo de titulación referido.

Guayaquil, Abril del 2014

La autora

_____

DANIELA ESTEFANIA MUÑOZ CEDEÑO

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

INGENIERÍA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL

AUTORIZACIÓN

Yo, DANIELA ESTEFANIA MUÑOZ CEDEÑO

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del proyecto titulado: "MONITOREO E IDENTIFICACION DE ATAQUES A REDES", cuyo contenido, ideas y criterios son de mi responsabilidad y autoría.

Guayaquil, Febrero de 2014

La autora

_____

DANIELA ESTEFANIA MUÑOZ CEDEÑO

AGRADECIMIENTO

A Dios por haberme dado la Ciencia y la Fe para concluir esta tesis, a mi familia que ha sido un pilar fundamental en el trascurso de mi vida, a mis amigos por siempre contar con ellos.

A nuestros profesores, por transmitir sus conocimientos, filosofías, dedicación y esfuerzo, por convertirnos personas profesionales e integras; a las autoridades de la facultad Técnica por la consideración y estimulo que nos han brindado en todo momento, y en especial al Decano, Director de carrera, Coordinador académico y a mi Director de Tesis por su ardua y valiosa colaboración, orientación en el desarrollo de la presente tesis.

DEDICATORIA

Este trabajo de tesis se lo dedico a mis padres Jerry y Magdalena gracias por todo su apoyo, y en especial a mi abuelo José Manuel que siempre tuvo fe en mí aunque en estos momentos él no pueda estar aquí pero yo sé que desde el cielo está muy feliz de mis logros, y solo quiero decirle que uno de sueños ya está cumplido y darle gracias por todo.

RESUMEN

El trabajo presente se desglosa por cuatro capítulos, que comprenden la identificación del problema, lo cual permite definir los objetivos y la hipótesis para su solución. En el primer capítulo se habla detalladamente del concepto de red, el monitoreo e identificación de la misma, se define los ataque que puede sufrir, quien o quienes son los atacantes y como se los conoce en el medio. En el segundo capítulo se analiza los tipos de ataques, sus formas de trabajo, que es lo que desea el atacante, como saber si existe un ataque y las vulnerabilidades que tiene el sistema operativo. En el tercer capítulo, se detallara todo sobre la seguridad de una red, como defenderse de un ataque y las medidas de seguridad que se debe tomar. En el cuarto capítulo se presentan las conclusiones y las recomendaciones.

ABSTRACT

This paper is broken down by four chapters, comprising identifying the problem, which allows you to define the objectives and hypotheses for their solution. In the first chapter discusses in detail the concept of network monitoring and identification thereof, may suffer the attack, who or who are the attackers and as they are known in the defined medium. In the second chapter the types of attacks, its working, which is what you want the attacker, such as whether there is an attack and vulnerabilities that have the operating system is analyzed. In the third chapter, detailing everything about the security of a network, such as defending against an attack and the security measures to be taken. Conclusions and recommendations are presented in the fourth chapter.

INDICE GENERAL

INDICE DE FIGURAS

INTRODUCCION

En nuestro planeta existen 2,300 millones de internautas y crecen constantemente las conexiones a internet, las redes se encuentran en constante peligro de ataques informáticos debido a que están conectados a esta red de comunicación, estos ataques son ocasionados por herramientas automáticas, lo cual ocurre cuando encuentran la vulnerabilidad y fallas en el diseño y configuración de una red (TCP, IPV4, WIFI, DNS, IP, APLICACIONES….) para de esta manera comprometer a la seguridad de la misma, la cual no ha tomado las medidas de seguridad mínimas .

Al conjunto de máquinas comprometidas y controladas remotamente por un ataque se les conoce como *Botnet*, normalmente se lo hace por medio de un IRC (*Internet Relay Chat*) y constituyen un negocio lucrativo donde operan verdaderas mafias, otorgándole la posibilidad al atacante de realizar ataques a gran escala desde todos los sistema infectados, la redes *Botnet* ofrecen al atacante o a los atacantes el anonimato, siendo los equipos *zombis* los que en última instancia están realizando el ataque o acción dañina.

En la actualidad pueden ser vendidas a terceras personas con intenciones diferentes a los del ataque original, en la actualidad el hallazgo de nuevas vulnerabilidades es más rápido que la capacidad de resolución de estas por parte de los fabricantes de *hardware* y *software*, muchas de las notificadas tardan meses en ser resueltas aunque muchos de estos problemas se pueden mitigar con la implantación de seguridad en la redes conectadas directamente a internet, algunas de ellas utilizando contrafuegos y arquitecturas más seguras .

Por estas razones es necesario realizar un constante monitoreo con Sistemas de Detección de Intrusos.

CAPITULO I GENERALIDADES

Este proyecto se basa en una investigación sobre el monitoreo e identificación de ataques a redes que consiste en un monitoreo e identificación, sobre el uso de antivirus, que es un ataque a una red, que se puede hacer ante un ataque a una red.

PROBLEMA

La falta o poca presencia de seguridad informática en un sistema operativo, aplicación, red o dispositivo, permite su intervención por parte de personas no autorizadas presentándose amenazas que representan un tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad representa el grado de exposición a las amenazas en un contexto particular, siendo indispensable establecer contra medidas que representan todas las acciones que se implementan para prevenir la amenaza.

OBJETIVO GENERAL

Caracterizar e investigar los elementos que intervienen en la seguridad en redes para mejorar la misma mediante instrumentos y protocolos de seguridad, de acuerdo a la necesidad de los usuarios que requieren mejor protección y privacidad de la información que circula en su red.

OBJETIVOS ESPECÍFICOS

- Conceptualizar las defensas físicas y operaciones de control como normas de prevención.

- Analizar las inseguridades que se presentan en las redes, tanto en los equipos como en los firewalls y en los sistemas operativos.

- Establecer estrategias de seguridad y caracterizar los estándares que existen para su elaboración.

- Caracterizar la piratería informática y su manera de operar para limitar lo más posible su acceso.

- Describir algunos elementos de seguridad que se pueden aplicar.

HIPÓTESIS

El tener un sistema monitoreado e identificado ayudará al usuario a tener un control de su red y de su equipo, permitiéndole al usuario saber cuándo denegar o aceptar una información de un equipo.

JUSTIFICACIÓN

Este trabajo de investigación pretende indicar algunos modelos para obtener una seguridad tolerable en los sistemas enlazados a una red, es decir una protección capaz de evitar que la mayoría de potenciales atacantes a los equipos informáticos tengan éxito en su agresión. No es posible certificar una total seguridad ante estos ataques, por ejemplo si es realizado por un técnico con experiencia, con bastante tiempo para su ejecución y siendo remunerado por su realización o que tiene interés en esos equipos, no le sería muy difícil el acceso. Lamentablemente esto es prácticamente inevitable, sin embargo es posible evitar que alguna persona ataque un equipo porque lo vio en una película o por información de una página web y pudo ejecutar un programa que no lo creó ni lo entiende.

El desarrollo que permite mejorar el nivel de vida de las personas incluye los aspectos tecnológico y de telecomunicaciones debido a la necesidad de interactuar entre los seres humanos para intercambiar básicamente información ya sea ésta pública o privada.

En el caso de la información privada se tiene la preocupación de que puedan robársela y utilizarla con fines lucrativos o para perjudicar a otros, razón por la cual es necesaria la seguridad en la transmisión de información, esto significa la adopción de medidas de prevención que eviten la penetración de personas no autorizadas en la red. (Bustamante)

El objetivo de esta investigación es la seguridad de las redes de computadoras para proteger la información que se está transmitiendo por una red, dicha seguridad puede ser física o lógica.

La seguridad física corresponde a la prevención de desastres naturales, inundaciones, terremotos, incendios, instalaciones eléctricas, etc. La lógica en cambio corresponde a las medidas para prevenir que personas no autorizadas accedan a la información, esto significa protegerla de los piratas informáticos, tales como los hackers, crackers, etc., aprovechando las vulnerabilidades de la red, por ejemplo de los sistemas operativos o la recepción de archivos desconocidos que pueden infectar sistema con virus u otros elementos. (Bustamante)

Técnicas y métodos utilizados en la investigación

- Método descriptivo permitirá explicar los fundamentos de la ingeniería utilizados en el análisis e identificación de ataques a redes, detallando las diferentes maneras más factibles para evitarlos.

- Método de investigación bibliográfica ya que se recopilará toda la información existente para detectar los problemas y soluciones que existen en los ataques contra la seguridad informática

1.1. ¿QUE ES UNA RED?

Atelin y Dordoigne (2006) expresa que:

Una red es un medio que permite a personas o grupo compartir información y servicios.

La Tecnología de las redes informáticas constituyen el conjunto de las herramientas que permiten a los ordenadores compartir información y recursos.

Las redes telefónicas forman una generación de redes de telecomunicación que precedió a la informática. La convergencia entre estos dos medios de comunicación es lo que se actualmente. De hecho, las nuevas tecnologías permiten el transporte de voz y datos con los mismos medios.

Una red está constituida por equipos llamados nodos. Las redes se categorizan en función de su amplitud y de su ámbito de aplicación.

Para comunicarse entre ellos, los nodos utilizan protocolos, o lenguajes comprensibles para todos ellos. (pg.10).

1.1.1 TIPOS DE RED

Existe de diferentes tipos

Red de área local (LAN):

Es un sistema de comunicación que permite que varios dispositivos independientes se comuniquen entre sí, una vez que exista una comunicación permitirá que se pueda realizar video llamadas, envió de datos, envió de información y cualquier otra forma de comunicación electrónica.

Topología

Al estar interconectados los distintos nodos de una red forman una figura y esa figura es la topología.

Tipos de topología de la Red LAN

Topología física y topología lógica.

La topología física.-

Gil- Pomares, Candelas (2010) define "la representación geométrica de todos de todos los enlaces de una red y los dispositivos físicos que se enlazan entre sí" (p.18.).

a) Las conexiones punto a punto es la comunicación que solo se realiza entre dos puntos son ellos dos, no existe un tercer punto.

b) Las conexiones multipunto la comunicación es diferente el punto central se comunica únicamente con los puntos remotos, y los puntos remotos con el punto central.

TIPOS DE TOPOLOLOGIA FISICA

Es la forma física como están distribuidos los ordenadores que la compone.

Existen varios tipos: es estrella, en bus, en anillo y topología hibridas.

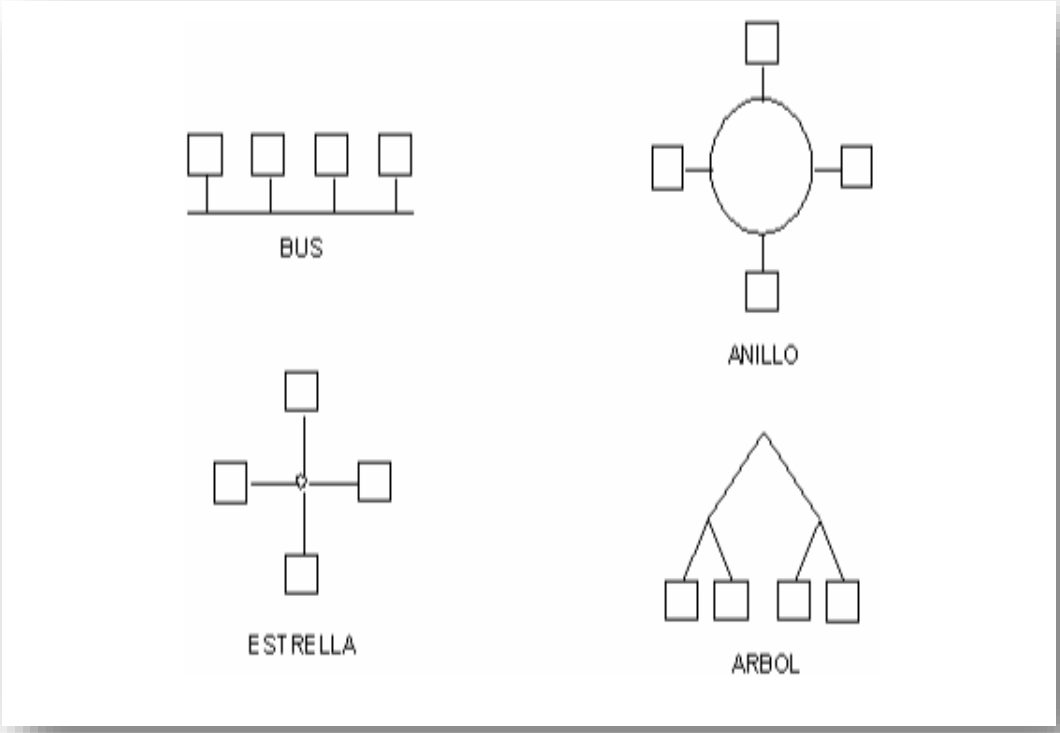


Figura 1.1.-Tipos de Topología física

Fuente: http://www.lsi.uvigo.net

a) Topologia estrella

Figura 1.2. - Topología Estrella

Fuente : http://www.ipviasatelite.com

Se la conoce como topología estrella porque tiene forma de estrella, tiene un nodo central que es se conecta con el resto de los nodos formando una estrella, cada estación tiene una conexión directa con un acoplador central.

Según su función, los acopladores se catalogan en:

Acoplador Pasivo: es la acción de trasladar físicamente a todas las líneas de salida la transmisión que se realizó o u efectuó al acoplador específicamente en una línea de entrada.

Acoplador activo: el acoplador tiene la capacidad de repetir y regenerar los bits que llegan a una línea de entrada en todas las líneas de salida debido a que por logia digital el acoplador ejerce una acción repetidora, excepto si se producen varias señales de entrada esto indicara que hay una colisión que va a producir una señal de salida para ser enviada hacia todas las líneas de salida.

Ventajas y Desventajas de la topología estrella

Ventajas

- El funcionamiento de la red no se verá afectado al producirse fallas en alguno de sus nodos.
- En comparación con otras topologías las averías en la topología estrella son fácil de detectar.
- La capacidad de proceso del nodo central permite conectar cualquier tipo de terminal, ya sean inteligente o no inteligentes.

Desventajas

- La red depende del nodo principal, es decir al dañarse esté afectaría a la red.
- Aunque las conexiones entre nodos no se necesitan grandes cantidades cables al estar lejos del nodo central requieren de gran cantidad de cableado.
- Dificultad en la expansión los nodos.
- La conexión a internet depende del buen funcionamiento del HUB o SWITCH
- El nodo central acto para soportar elevadas cargar de tráfico.

b) Topología bus

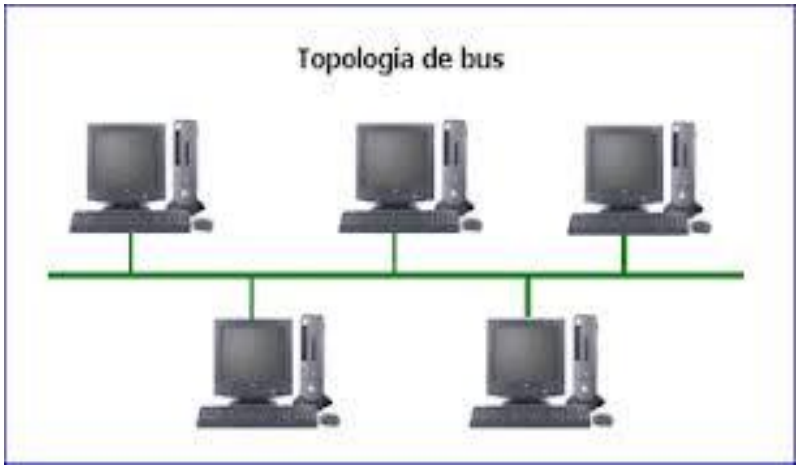


Figura 1.3. - Topología bus

Fuente: http://www.ecured.cu/index.php/Archivo:Bustopology.jpeg

A diferencia de la topología estrella la topología bus se caracteriza por no tener nodo central ya que estos comparten el mismo circuito de una manera continua, es decir uno a continuación del otro, además se sirve de terminadores que son dispositivos colocados en los extremos del bus cuya función es permitir que la información se la reciba en todas las estaciones, para que cumpla su función es necesario que los terminales cuenten con todos los elementos de una red. Al cable con todos estos elementos se lo denomina BACKBONE.

Es muy importante resaltar que la topología bus los nodos tiene un tiempo de espera para transmitir la información evitando de esta manera se produzca choques o interferencia con la transmisión de otra información.

Ventajas y Desventajas

Ventajas

- Su velocidad para trasmitir la información es de 10Mbps.
- Si un ordenador falla no se vería afectada la comunicación.
- Cuenta con terminales que evitan rebotes de la señal.
- Moderada cantidad de cableado para la conexione.
- Permite incluir de manera fácil nuevos ordenadores incrementando la red.

Desventajas

- Amenaza al funcionamiento del sistema de manera parcial o total en el cableado en el caso de que se produzca una falla en el cableado.
- Dificultad para situar las averías dadas en esta topología.
- Solo se permite en esta topología nodos inteligentes.
- Da facilidad al ataque de que pueda interceptar en la red, debido a que la información es bidireccional.

c) Topología anillo

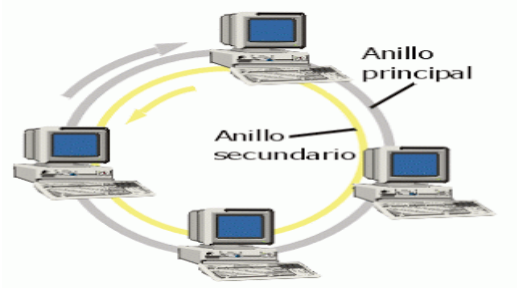


Figura 1.4. - Topología anillo

Fuente: http://wo0crazhita.blogspot.com/2011/06/topologias.html

Se caracteriza por su forma de anillo, formada por las estaciones; están conectadas por un cable común, su tipo de conexión es punto a punto, por su forma permite que la señal circule en una sola dirección, en esta Topología la información es examinada por cada nodo hasta llegar al nodo correspondiente.

Ventajas y Desventajas

Ventajas

- Al ser unidireccional permite la utilización de fibra óptica permitiendo alta velocidad.
- Facilidad en la conexión de nuevos nodos.
- Mínimas posibilidad de congestionamiento.

Desventajas

- Complejidad en el cableado.
- Al existir un fallo en un nodo toda la conexión se ve afectada.
- Dificultad para localizar los problemas, daños o fallos que se presenten.

d) Topología híbrida

La Topología también conocida como Topología mixta, se sirve de las topologías entes mencionadas en este trabajo para formar una red completa, es la más utilizada de una de sus ventajas es que si un equipo falla no afecta al resto de la red.

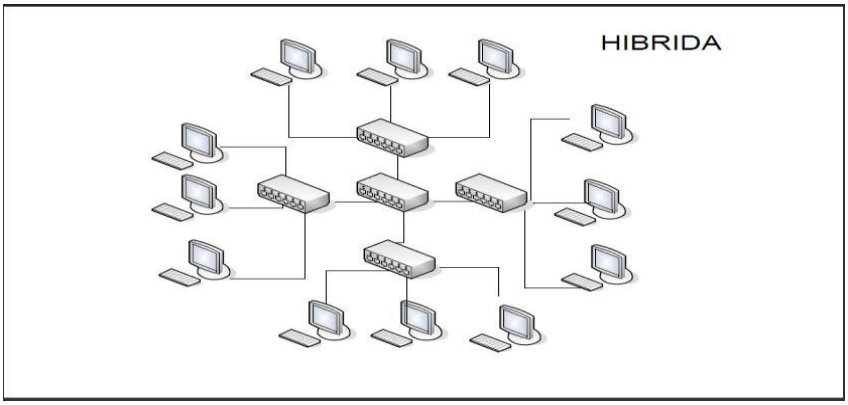


Figura 1.5. - Topología Hibrida

Fuente: http://alemorenoredes.blogspot.com/2010/04/t.html

La topología en árbol esta Topología es el resultado de la unión de Topología estrella y bus, presenta la forma de un árbol con un nodo de enlace troncal que permite una serie de ramificaciones por donde se trasmite la información a partir de la raíz o punto estrella , contiene un concentrador central y un concentrador secundario; el concentrador central sirve para controlar el tráfico de la red, no obstante se encuentra conectado a dicho concentrador el concentrador secundario en el cual se conectan a los dispositivos que no conectaron al concentrador central.

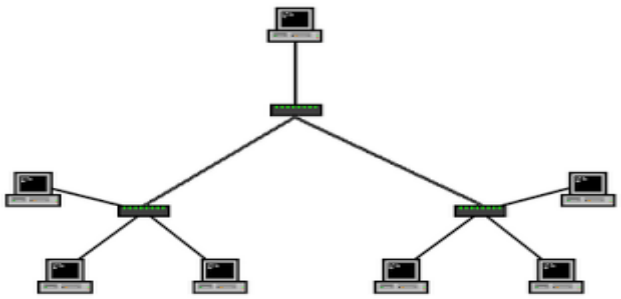


Figura 1.6.- Topología Árbol

Fuente: http://toparbol.blogspot.com/

Ventajas y Desventajas

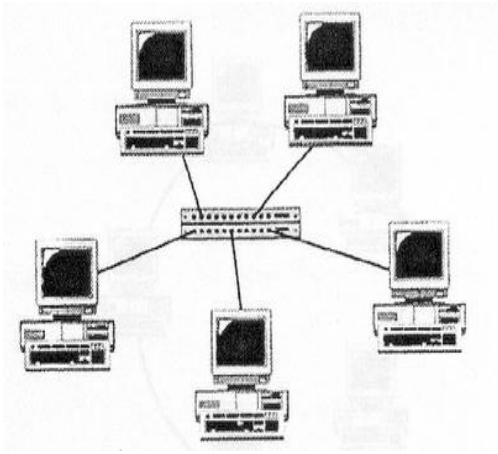
Ventajas

- Facilita la expansión de la red.
- Bajo grado de complejidad para detectar problemas o daños.
- Por su característica ramificada en caso de avería no es apagar toda la red, ya que se pueden desconectar estaciones o ramas completas hasta encontrar el problema.

Desventajas

- Dependencia total de línea principal
- Al estar conectadas todas las ramificaciones a una línea principal, las convierte dependientes de esta.
- No siempre la señal es de calidad debido a las distancias, cuando la señal no es buena es necesario el uso de repetidoras.

Topología anillo-estrella.- como su nombre lo indica es la fusión de la Topología estrella y anillo, contiene un nodo central cuyos forman una red en anillo.



1Figura 1.7. - Topología Anillo- Estrella

Fuente: http://redes-angela.blogspot.com/2010/12/anillo-en-estrella.html

Ventajas y Desventajas

Ventajas

- Tiene las ventajas de la Topología estrella y anillo.
- Su Topología permite que en el caso de que un equipo falle el resto de la red no se vea afectada.

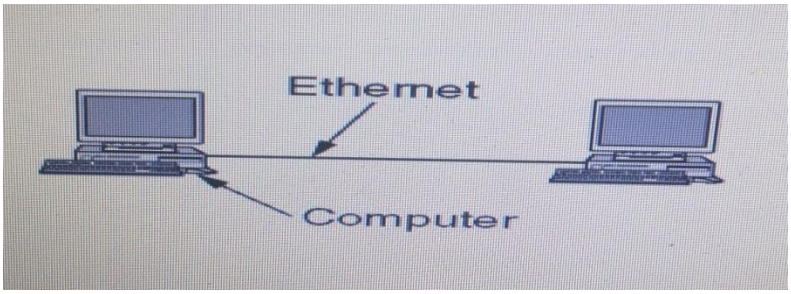
Desventajas

- Por su Topología presenta dificultad en su complejidad.

La topología lógica

Es la que necesita de una estructura física para la comunicación de las estaciones, no es necesaria la precesión de cables ya que existe una conexión inalámbrica.

Broadcast (Ethernet).- se basa en que cada ordenador envía sus datos hacia todos los demás del medio de red. Las operaciones se realizan por orden de llegada como si fuese Ethernet.



2Figura 1.8. - Topología Broadcast

Fuente: http://www.ie.itcr.ac.cr/faustino/Redes/Clase8/4.2Ethernet.pdf

Transmisión de Tokens.- El acceso a la red es controlado mediante la transmisión de un Token electrónico (serie especial de bits) a cada equipo de forma secuencial a cada host. Cuando un host recibe el Token se le permite enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el Token al siguiente host ya que existe sólo un Token por cada red.

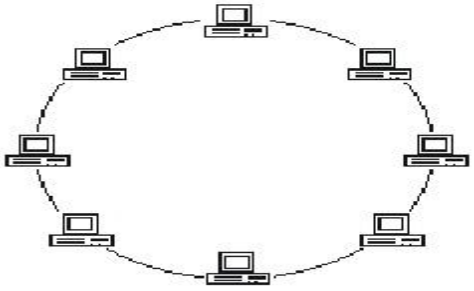


Figura 1.9.- Transmisión Token

Fuente: http://www.scribd.com/doc/13908677/Topologia-Logica

Red de área metropolitana (MAN)

Se caracteriza de varias LAN las mismas que deben tener una ubicación geográfica cercana cuya distancia debe ser de 50km, presenta un estándar equivalen a la norma IEEE, con una cobertura de banda ancha para satisfacer las necesidades en área urbanas, atreves de múltiples servicios ofrecidos por el internet.

Como medio de transmisión utiliza la fibra óptica y par trenzado que permiten crear nuevas redes metropolitanas con varias velocidades que oscilan entre 2Mbits/s hasta 155 Mbits/s.

Según Herrera (2003) "la MAN es un red cuyo diámetro no va más allá de 50km y responde claramente a la necesidad de un sistema de comunicación de tamaño intermedio con beneficio que puedan ofrecer LAN O WAN" (pág. 65).

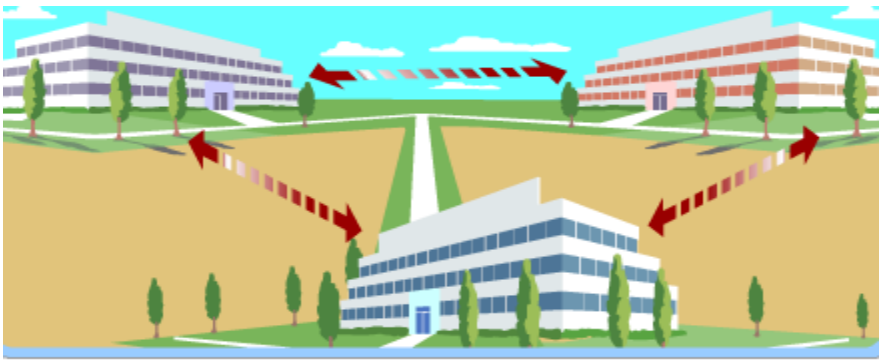


Figura 1.10.- Red MAN

Fuente: http://www.librosvivos.net

Razones por las cuales es necesaria una Red MAN

- **Ancho de banda:** debido a su amplia cobertura su utilización es muy frecuente.
- **Nodos de red:** por superar los 500 nodos de acceso de red su eficacia tanto como en lugares públicos como en privados.
- **Extensión de red:** para una red metropolitana se considera que un diámetro de 50km es suficiente para la cobertura deseada.
- **Distancia entre nodos:** Esta red permite distancia entre nodos de acceso de varios kilómetros, debido a sus distancias se pueden conectar edificios o campus privados.
- **Trafico en tiempo real:** una de las bondades de la red es permitir el acceso a la red en un tiempo casi real, es decir la información puede llegar sin retraso pese a que la carga de la red puede ser elevada.
- **Integración de voz, video y datos:** la integración de Servicios síncronos que ofrece el internet dependen de una reserva del ancho de banda para el tráfico multimedia lo que obliga a que las redes del área metropolitanas se presenten de forma óptima.
- **Disponibilidad:** la red metropolitana tiene la facultad de detectar cualquier fallo que en encuentre en un nodo o cable aislando para recuperar la operación de manera exitosa.
- **Alta fiabilidad:** permite controlar con alto grado de fiabilidad en entornos donde el índice de errores es alto como es el tráfico aéreo, la fibra de óptica nos permite que la tasa de error mínima a comparación con la del cobre la cual

a pesar de tener la misma longitud y tasa de error no detecta los errores evidenciándose un orden que va de 10-20.

- **Alta seguridad:** la seguridad que brinda la red metropolitana se debe a que para su transmisión utiliza la fibra óptica la misma que imposibilita la lectura o cambio de la señal óptica puesto a que estas acciones interrumpirían el enlace produciendo su caída temporalmente.
- **Inmunidad al ruido:** por la interconexión de redes de área local y redes de alta velocidad eliminando todo tipo de barrera tecnológica.
- **Protocolos de comunicación:** la comunicación de nodos está dada por una serie de reglas y procedimientos que están dados en diferentes niveles de comunicación, que son: nivel 1, nivel 2 y nivel superior bajo la jerarquía OSI.

Ventajas y Desventajas

Ventajas

- Bajos costos de explotación comparada con otras redes.
- Seguridad por su uso de fibra óptica.
- La transmisión de trafico una red MAN no requiere de un ancho de banda fijo.
- El ancho de banda que ofrece la MAN es superior en comparación con otras redes.

Desventajas

- Presenta ciertas limitaciones en aspectos legales y políticos que puede incidir en la decisión del comprador de la red.
- La cobertura no supera los 50km de diámetro.

Red de área amplia (WAN)

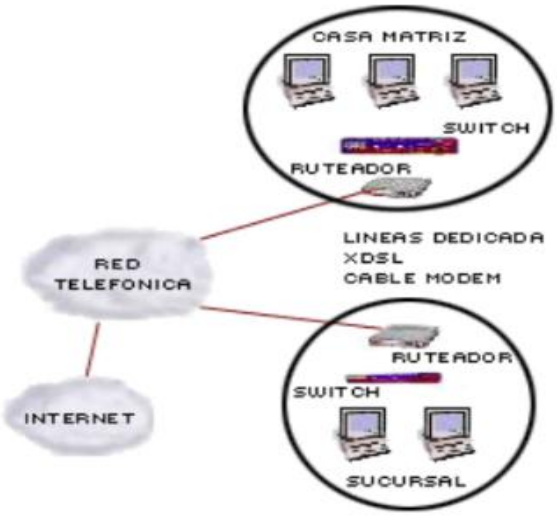


Figura 1.11.- Red WAN

Fuente: http://dspace.ups.edu.ec

La conectividad que brinda la red WAN es excelente, ofreciendo una cobertura 100 y 1000 km de distancian, beneficiando a grandes ciudades y en algunos casos a un país entero, este tipo de red podemos encontrar en empresa pública o privada; también existen proveedores de internet que la utilizan para proveer de este servicio a sus clientes.

El acceso a internet y la conexión de sitios de otras entidades que la ofrece la red WAN son suministrados por una operada que le permiten a la WAN dar servicios de varios tipos trafico siendo los más generalizados los de datos y telefónicos.

La importancia de este tipo de red se debe a que permite estable conexión en lugares remotos, simplifica fronteras espacios geográficos.

Ventajas y Desventajas

Ventajas

- La red WAN permite el acceso a archivos desde cualquier sitio.
- Alta capacidad de velocidad.
- Cubre grandes áreas geográficas.
- Permite la utiliza la utilización de un software especializado

Desventajas

- Existen compañías telefónicas y servidores de internet que afectan al diseño y funcionamiento de la WAN.
- Susceptibilidad de error en las líneas.
- Elevados costos para la adquisición de enlaces.
- La rapidez de acceso depende de la capacidad de memoria.
- Vulnerabilidad frente ataques.

Tipos de Redes WAN

Los tipos de redes WAN son las siguientes:

- **Redes dedicadas.-** están dadas por una línea para el tráfico del usuario no necesita de un nodo intermediario, se sirve de dos puntos, donde estable una conexión permanente siendo esta rápida brindando mayor seguridad.
- **Redes conmutadas.-** a diferencia de las redes dedicas las conexión entre dos puntos no es necesaria y se clasifican de la siguiente manera:

- **Conmutadas de circuitos.-** la comunicación se la efectúa a través de una llamada que le permiten al usuario una conexión directa.
- **Conmutadas por Paquetes.-**. suele servirse de un computador en el cual se encuentra conectado a una serie de terminales que reciben la información para que el conmutador examine la dirección del mensaje. El usuario tiene varias opciones frente al mensaje recibido.

- **Redes Públicas.-** son configuradas para el uso público ya que no cuenta con contraseñas, y los usuarios las adquieren a través de suscripción.
- Los usuarios se pueden suscribir a través de diversas compañías ya sean de comunicación local o a larga distancia
- **Red Pública de Conmutación Telefónica (PSTN).-** utilizan un circuito tradicional, el circuito se mantiene abierto hasta que la persona cuelgue la llamada, en tiempo real garantizando la calidad de voz.
- **Redes privadas.-** dependen de la entidad a la que le presta servicio para lo cual es necesario destacar los siguientes aspectos.
  - El proveedor de internet requiere que se utilice sus propios equipos.
  - Permite al proveedor de internet utilizar los recursos de la red de la manera que le favorezca.
  - Pese al alto costo de la red privada las compañías las utiliza a su sistema de seguridad y alto nivel garantía que estas ofrecen.

Topología de la red WAN

Hablar de Topología es referir a la forma gráfica que tiene las estaciones de transmisión.

Existen numerosas topologías con diversos funcionamientos, costos y escalas.

Existen dos tipos de Topología:

- Topología física.- en este tipo de Topología lo importante es el patrón con lo que están formados los nodos que están en conexión con la red, no es necesario puntualizar qué tipo de dispositivo se está utilizando la manera o la forma en que se realiza la conexión o el destino en la red.
- Topología lógica.- describe la conversión de los datos a un formato especifico y los procesos que se aplican en la transmisión de los pulsos eléctricos.

Topología punto a punto de la red WAN

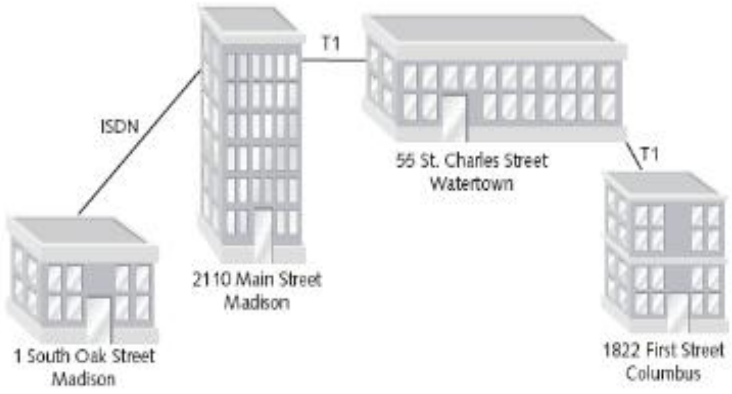


Figura 1.12.- Topología punto a punto

Fuente: http://dspace.ups.edu.ec

La Topología WAN se conecta un nodo con otro nodo pro medio circuitos que permiten la comunicación, para que las pequeñas empresas arrienden los canales, y se produzca la produzca la comunicación entre los dos puntos.

Topología anillo de la red WAN

Conecta diversos nodos, que están ubicados en distinto lugares para formando un anillo.

La Topología presenta como ventaja sobre P2P (arquitectura la comunicación) , que la red no se ve afecta frente a un problema detectado por un nodo, puesto que los repetidores tienen la capacidad de repetir los datos a otro repetidor , incluso en el caso de que un repetidor llega muy cargado de información.

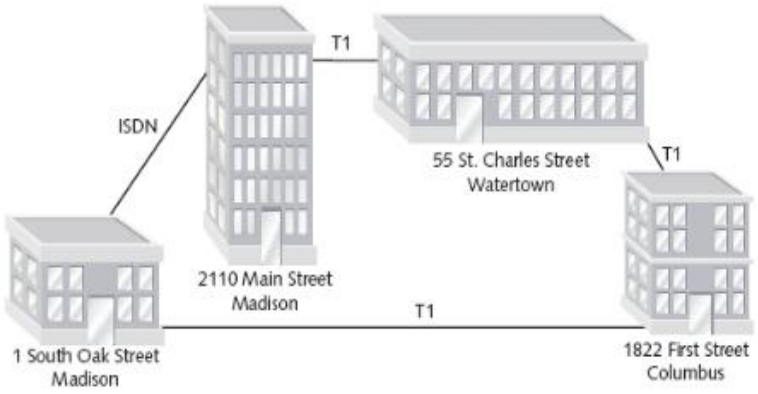


Figura 1.13.- Topología de la red WAN

Fuente: http://dspace.ups.edu.ec/

Topología estrella de la red WAN

La característica principal es el punto principal de conexión para los diferentes puntos, formando una estrella, que son rutas verdaderas para él envió de datos. Cabe recalcar que la confiabilidad que brida la Topología estrella de la red WAN es superior a los WANS de anillo.

Esta Topología ayuda que la trayectoria que recorren los datos sea más corta.

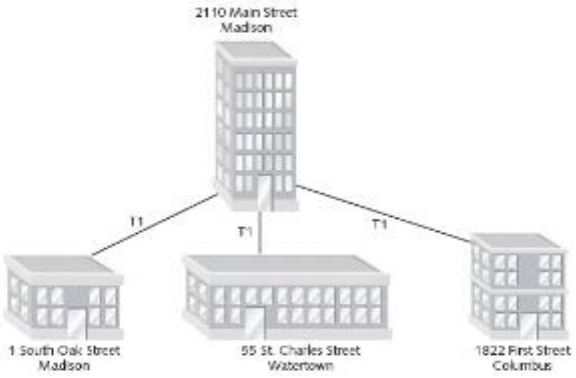


Figura 1.14.- Topología Estrella

Fuente: http://dspace.ups.edu.ec

Topología malla de la red WAN

Al interconectar los nodos forman una maya, que permiten que los datos se dirijan de una forma directa a sus destino, si surgen un problema en una conexión el resto de la red no se verá afectada porque los repetidores tiene la capacidad de volver a enviar la información de manera rápida debido que esta topología cuenta con múltiples rutas para que los datos lleguen a su destino.

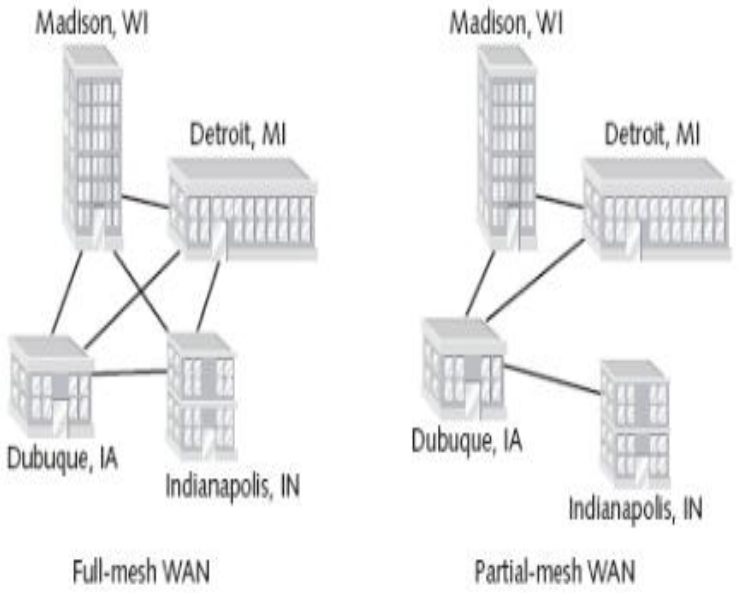


Figura 1.15.- Topología malla

Fuente: http://dspace.ups.edu.ec

Topología Tired de la red WAN

Esta topología facilita el crecimiento de la red debido a la fácil inclusión y acoplamiento de los puntos de interconexión, que se presentan organizados en capas, conectados en diferentes niveles, la ubicación de los sitos WAN forman una estrella o un anillo.

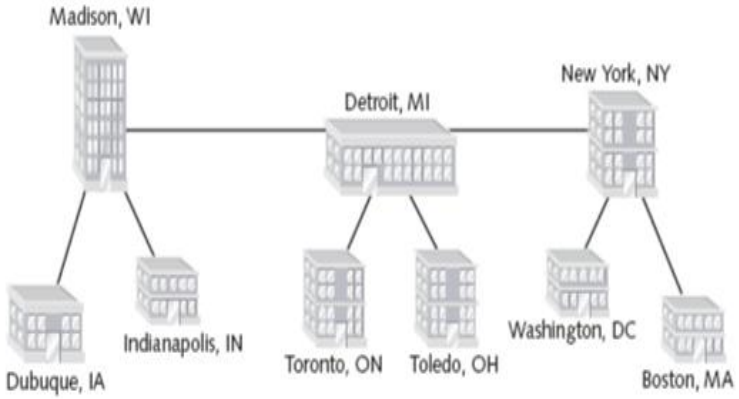


Figura 1.16.- Topología Tired

Fuente: http://dspace.ups.edu.ec/

1.2 ¿QUE ES UN MONITOREO A UNA RED?

Es la actividad por medio de la cual se controla y verifica si existen o no anomalías en una red, para un efectivo monitoreo se hace necesario que tenga una buena configuración de software de modo que la red esté actuando con normalidad.

El monitoreo de la disponibilidad de red.

Tiene como finalidad verificar los servicios dados por el servidor funciona de manera correcta y que los usuarios no tenga problemas al ingresar a la red.

Incluyendo el monitoreo de páginas web, servidores de correo electrónico, y conexiones de internet.

El monitoreo del ancho de banda y la velocidad de red.

Permite que cual carga o descarga electrónica se realice sin demora.

Las cargas son evaluadas verificando la utilización de estas.

Cada dispositivo tiene un alcance diferente que deben ser definidos al momento del monitoreo.

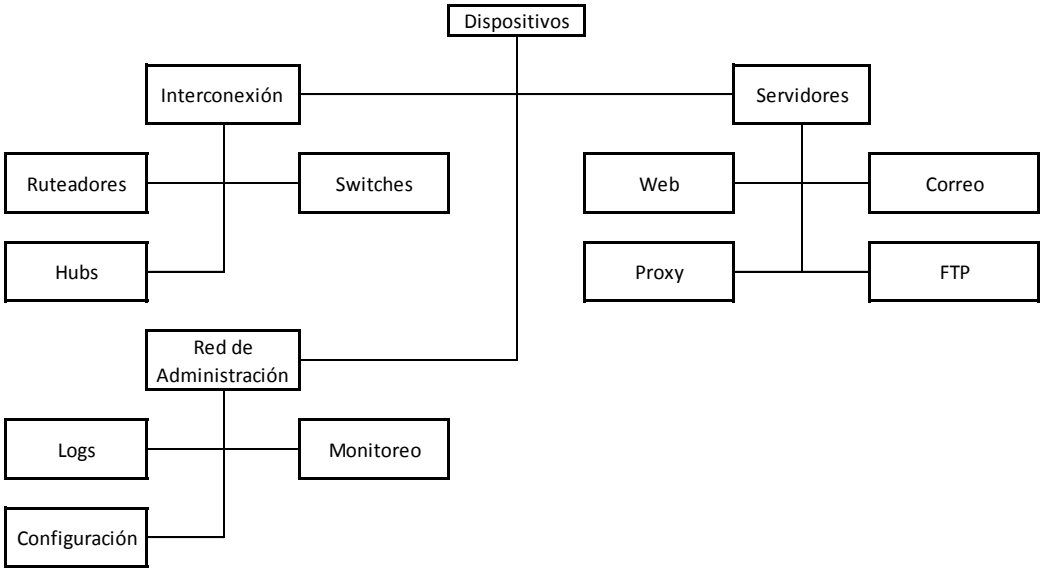


Figura 1.17.- Dispositivos que son monitoreados

Elaborado por: Autora

Existen diferentes tipos de monitoreo, se los puede dividir de la siguiente manera

1.2.1MONITOREO PASIVO

Este enfoque se basa en la obtención de datos de recolectar y analizar el tráfico que circula por la red. Se emplean diversos dispositivos como Sniffers, ruteadores, computadoras con software de análisis de tráfico y en general dispositivos con soporte para snmo, rmon y netflow.

Técnicas de Monitoreo: Solicitudes remotas

Mediante SNMP

Se utiliza esta técnica para el informe estadístico sobre el uso de ancho de banda en la red el cual se logra. Este informa se con el acceso a los dispositivos de dicha red.

Esta técnica de monitoreo generara paquetes traps si llegara a producirse sucesos iniciales.

Captura de tráfico

Según en su tesis titulada Estudio de las técnicas de análisis de flujos IP y su aplicación en el monitoreo de redes de datos en la Escuela de Ingeniería en Sistema perteneciente a la FIE consideran que: "Se puede la realizar de las siguientes maneras:

1) Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que recibe en un puerto hacia otro donde estará conectado el equipo que realizara la captura.
2) Mediante la instalación de un dispositivo intermedio que captura el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra (pag. 23)."

Análisis de tráfico

Según Anabelen Romero y Escudero Andi (2009) en su tesis titulada Estudio de las técnicas de análisis de flujos IP y su aplicación en el monitoreo de redes de datos en la Escuela de Ingeniería en Sistema perteneciente a la FIE consideran que: "Tiene como propósito detectar las aplicaciones de uso más frecuente a través de un dispositivo intermedio que contenga una aplicación capas de clasificar el trafico existente en la red (pag.24)."

Flujos

Según Ana Belén Romero y Escudero Andi (2009) en su tesis titulada Estudio de las técnicas de análisis de flujos IP y su aplicación en el monitoreo de redes de datos en la Escuela de Ingeniería en Sistema perteneciente a la FIE consideran que: "También utilizado para identificar el tipo de tráfico utilizado en la red. UN flujo es un conjunto de paquetes con.

- La misma IP origen y destino
- El mismo puerto TCP origen y destino
- El mismo tipo de aplicación.
- Los flujos pueden ser obtenidos de tuteadores o mediante dispositivos que sean capaces de capturar tráfico y transformarlo en flujos. También es usado para tareas de facturación (billing) (pg.24). "

1.2.2 MONITOREO ACTIVO

Se utiliza para esta clase de monitoreo paquetes de prueba que deben ser inyectados en la red, con el propósito de medir el tiempo de respuesta de información.

Benjamín C. y Bermúdez A. (2012) en su investigación sobre Cableado estructurado dice:

"Técnicas de monitoreo activo

- ICMP: Diagnosticar problemas en la red.
- Detectar retardo, perdida de paquetes.
- RTT: Disponibilidad de host y redes.
- TCP: Tasa de transferencia
- Diagnosticar problemas a nivel aplicación
- UDP: Perdida de paquetes en un sentido (one -way) RTT (traceroute) (pág. 40)."

1.2.3 ALARMAS

Altamirano C (2005) considera que:

Las alarmas don consideradas como eventos con comportamiento inusual. Las alarmas más comunes son las que reportan cuando el estado operacional de un dispositivo o servicio cambia. Existen otros tipos de alarmas basado en patrones previamente definidos en nuestras métricas, son valores máximos conocidos como umbrales o Threshold. Cuando estos patrones son superados

se produce una alarma, ya que es considerado como un comportamiento fuera del patrón. Algunos tipos de alarmas son:

- Alarmas de procesamiento.
- Alarmas de conectividad.
- Alarmas ambientales.
- Alarmas de utilización.
- Alarmas de disponibilidad (estado operacional) (pg.13).

1.2.4 HERRAMIENTAS PARA RESOLVER PROBLEMAS DE MONITOREO DE RED

Adelaida Amaya (2006) en su tesis sobre IPMONITOR Y CACTI considera que (Cacti Es un programa de monitoreo grafico de redes, el cual nos ayuda a elegir unas correcta solución a algún improvisto que surja en la red que administra. El entorno grafico hacia los usuarios (Fontend), es realizado en PHP y se maneja con base a una base de datos de MySQL, también tiene otros programas que le dan un correcto funcionamiento. (pag 44))

- **Cacti.-** A través de RRDT permite que los usuarios grafique la cara de la CPU al mismo tiempo monitorearla, el Cacti se basa de sus funciones gráficas y de la información de sus dispositivos. Se la utiliza en la recopilación de datos, permite identificar el perdió de servicio establecido y presenta una gráfica de los resultados, el servicio de alarma es otra característica de esta herramienta la cual la utiliza a través de umbrales.

- **Net-SNMP.-**

  Acosta Luis (2006) en su trabajo sobre Net-Snmp concluye que "NET-SNMP es un conjunto de aplicaciones usado para implementar el protocolo SNMP usando

  IPv4 e IPv6. Incluye:

  – Aplicaciones de línea de comandos para:

  - Tomar información de dispositivos capaces de manejar el protocolo SNMP, ya sea usando peticiones simples (snmpget, snmpgetnext) o múltiples (snmpwalk, snmptable, snmpdelta).
  - Manipular información sobre la configuración de dispositivos capaces de Manejar SNMP (snmpset).
  - Conseguir un conjunto de informaciones de un dispositivo con SNMP (snmpdf, snmpnetstat, snmpstatus).
  - Traducir entre OIDs numéricos y textuales de los objetos de la MIB, y mostrar el contenido y estructura de la MIB (snmptranslate).

  – Un navegador gráfico de la MIB (tkmib), usando Tk/perl.

  Las notificaciones seleccionadas pueden guardarse en un log (como syslog o un archivo de texto plano), ser reenviadas a otro sistema de gestión de SNMP, o ser pasadas a una aplicación externa. (Pg.3-4).

- **Nagios.-** se convierte en un vigilante de los servicios y de los hots dando alerta frente a la presencia de problemas o dificultades y también cuando estas reciben solución; por ser muy flexible tiene la capacidad de adaptarse a diferentes situaciones.

1.2.5 TOPOLOGIA DE UN SISTEMA DE MONITOREO

Contiene un servidor SNMP que utiliza al Protocolo SNMP y a los dispositivos para hacer solicitudes, envía la respuesta solicitada canalizada por un agente SNMP.

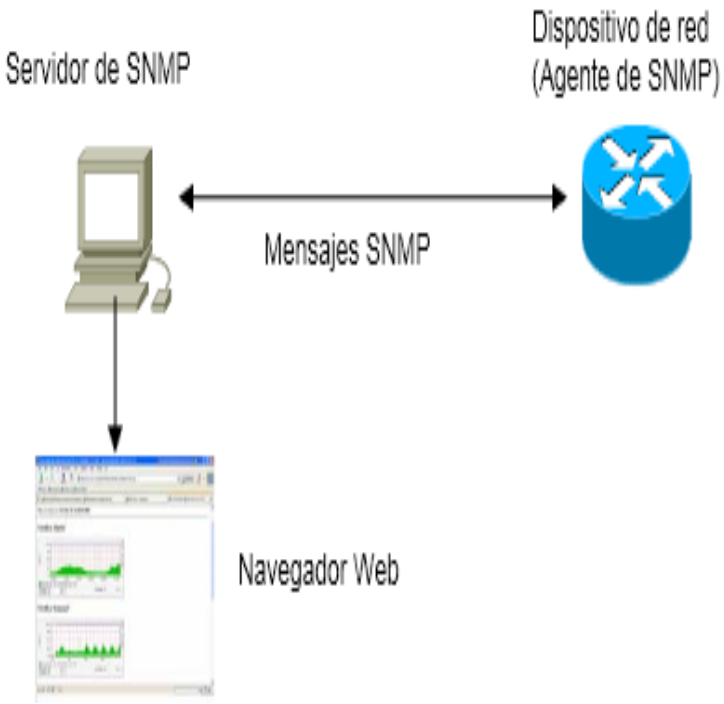


Figura 1.18.- Solicitudes Mediante SNMP

Fuente: http://juliorestrepo.files.wordpress.com/

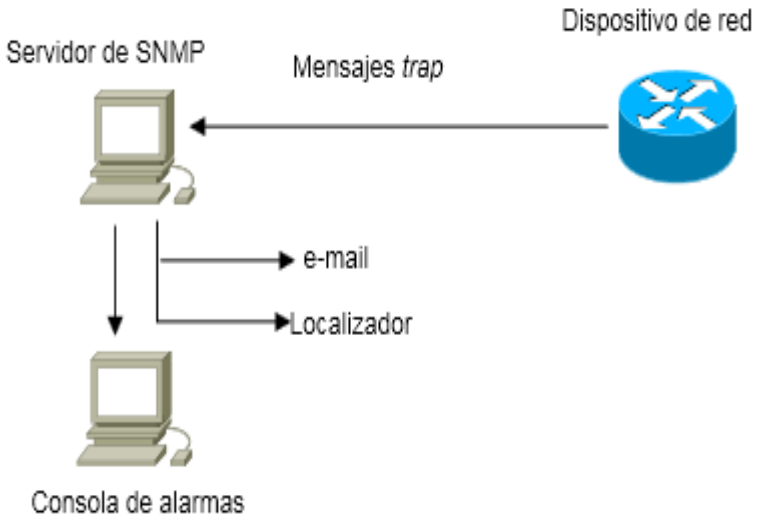


Figura 1.19. - Envió de traps

Fuente: http://juliorestrepo.files.wordpress.com

1.3 ¿QUE ES UNA ATAQUE A UNA RED?

Madrid Nicolás (s.f.). Expresa que:

"Un ataque consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño."(pg.4)

Es la forma por la cual el intruso logra ingresar a un sistema, con intenciones desconocidas, aprovechándose de la vulnerabilidad que este tiene.

En algunas ocasiones estos ataques se extendiendo a lo largo de la red.

Consecuencias:

Existen muchos daños que puede originar los virus en un sistema operativo entre ellos tenemos:

- **Daños triviales.-** los virus pueden ser eliminados en minutos por la facilidad que presentan para ser removidos.
- **Daños menores**.- virus Jerusalén conocido como viernes 13 forma parte de este tipo de daños tiene la característica que puede borrar cualquier información e incluso programas que el usuario dese utilizar, frente a estos daños tendrá que volver a instalar estos programas.
- **Daños moderados.-**para que se produzca este daño el virus debe formatear el disco duro y también puede mesclar los componentes de ubicación de archivos o también puede llegar a ocasionar daños en el disco duro sobrescribiendo el disco duro dañando el sistema operativo obligando al usuario a reinstalarlo y utilizar el respaldo ósea el backup operación que se la realiza aproximadamente en una hora.
- **Daños mayores.-** este daño no se lo nota y en algunas ocasiones desconocemos de su existencia, contamina tanto nuestro sistema que puede dañar nuestro backup. Como ejemplo podemos tomar el virus Dark Avanger que actúa acumulando los archivos para reescribir la información de un sector que lo escoge al azar.
- **Daños severos.-** en este daño los virus pueden camuflar la información debido hay mínimos y progresivo, el usuario los puede pasar desapercibidos porque los daños no se pueden detectar con facilidad.

- **Daños ilimitados.-** en este tipo de daños el virus obtiene muchos privilegios, incluso puede entrar en el sistema y hacer lo que quiera, programas como CHEEBA, VACSINA.44. LOGIN Y GP1 entre otros son los responsables de estos destrozos.

CAPITULO II ANÁLISIS DE UN ATAQUE A UNA RED

En este capítulo se procederá a analizar los ataques que pueden existir en un Red, las formas de los ataques, los efectos que, quienes son los atacantes, los objetivos de los atacantes y las razones de los atacantes.

2.1 TIPOS DE ATAQUES A LA RED

2.1.1 ATAQUE DE REPETICION

Se produce cuando una secuencia de mensajes, es copiada por un atacante, lo que genera una sucesión de mensajes que aparentan ser legítimos pero que en realidad generan resultado negativos, como una demanda excesiva de un elemento.

APLICACIÓN

SUPLANTACION DE INDENTIDAD

Este ataque consiste en la captura de información y él envió de esta para suplantar la identidad de la víctima, es de conocimiento general que intercambio de claves de protocolo criptográfico que en su génesis fue muy susceptible por ataques de inyección lo cual es posible evitar con una aplicación adecuada de esquema de protocolos criptográficos.

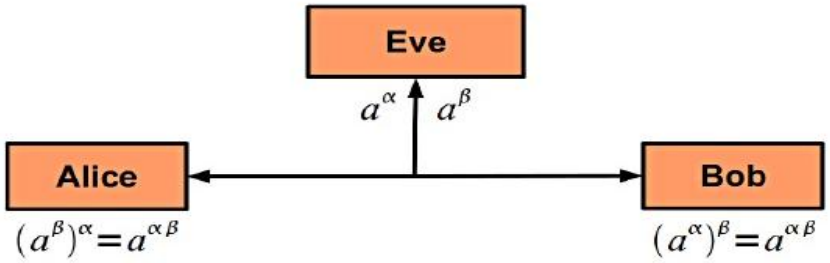


Figura 2.1.- Protocoló de Diffie-Hellman

Fuente: http://www.slideshare.net/fivefingers/protocolo-de-diffiehellman

NEGACION DE SERVICIO

Este ataque se produce cuando hay una sobre carga de mensajes debido al ataque de replay, lo que hace que este deje de funcionar correctamente.

Este tipo de ataque se lo puede evitar ya que los routers tienen la capacidad de receptar la información que ya ha sido utilizada para ser descartada, y dándole a los mensajes que si tiene valides un tiempo de caducidad para que los routers los eliminen.

2.1.2 ATAQUE MAN IN THE MIDLE

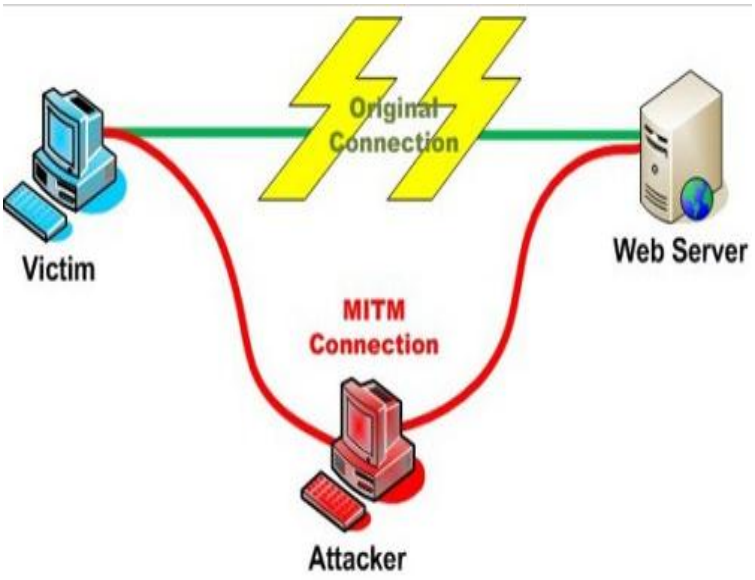


Figura 2.2. - Ataque MAN-IN –THE-MIDLE

Fuente: http://blog.sangregorio.edu.ec

Esta clase de ataque se viola la privacidad cuando dos personas entablan una conversación vía internet, el atacante se introduce en dicha conversación, puede tener la opción de no solo leer los si no cambiarlos y en muchos casos introducir otros nuevos sin que las víctimas se den cuenta, este ataque lo puede hacer una manera sencilla en una red Wi-fi sin dejar evidencias.

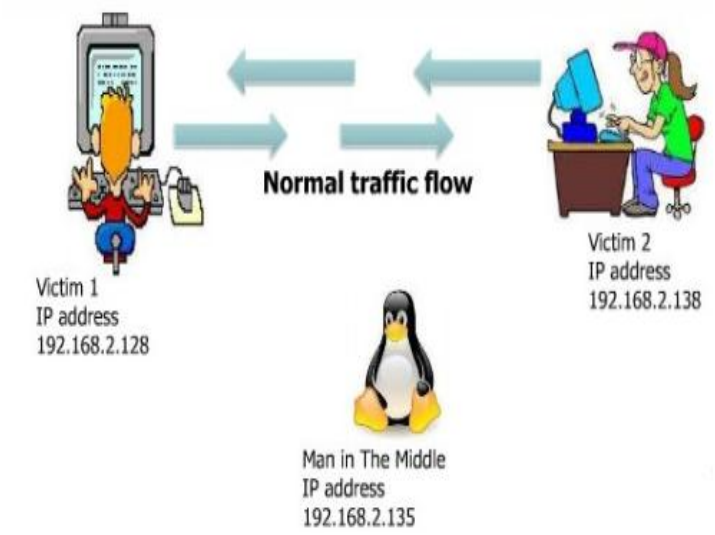


Figura 2.3.- Comunicación antes de un ataque Man in the middle

Fuente: http://seguridadpcs.wordpress.com

La figura representa a tres actores Daniela y Daniel que desean comunicarse y aparece Sebastián (Man in the middle) que es el que se propone violar la privacidad de esa conversación interceptándola , para poder cumplir con objetivos que pueden ser aparte de leer los mensajes, modificarlos o enviar nuevos mensajes falsos haciéndose pasar por uno de ellos.

En esta conversación Daniela “el intruso” le pide a Daniel que le envié su IP, si Daniel acepta petición y se la envía Sebastián ósea el intruso tendrá acceso a la información de Daniel.

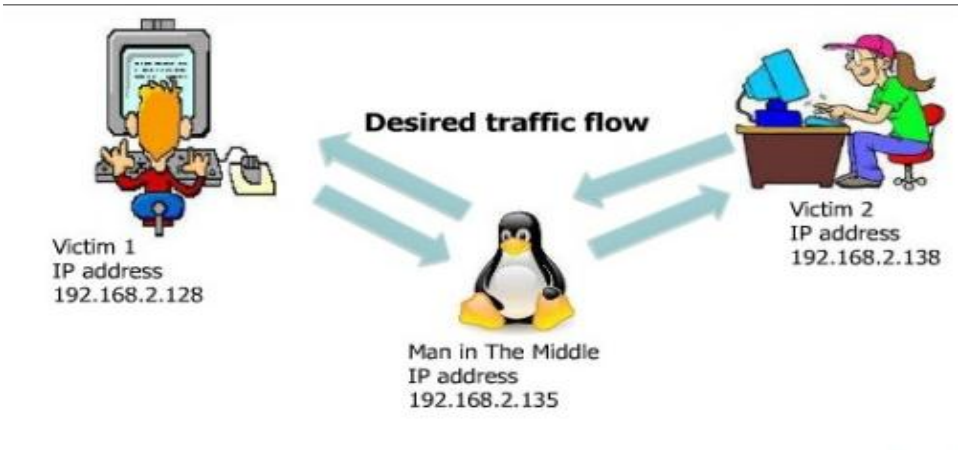


Figura 2.4.- Comunicación después de un ataque man in the middle

Fuente: http://seguridadpcs.wordpress.com

Posibles sub ataques.

Madrigal Edith (2011) expresa que:

El ataque MitM puede incluir algunos de los siguientes sub ataques:

*Intercepción de la comunicación (eavesdropping), incluyendo análisis del tráfico y posiblemente un ataque a partir de textos planos (plaintext) conocidos.

*Ataques a partir de textos cifrados escogidos, en función de lo que el receptor haga con el mensaje descifrado.

*Ataques de sustitución.

*Ataques de repetición. (pag.4)

2.1.3 ATAQUE DE REPETICION DE PAQUETES ARP

Los vectores de inicialización son generados al momento de generar ataques de repetición de paquetes ARP

Siendo útiles en el siguiente caso.

- La retransmisión de un nuevo IV se por escuchar paquetes ARP y luego transmitirlos al AP.
- Se permite obtener la clave WEP por la retransmisión repetida del paquete ARP en conjuntos con los IV nuevos.

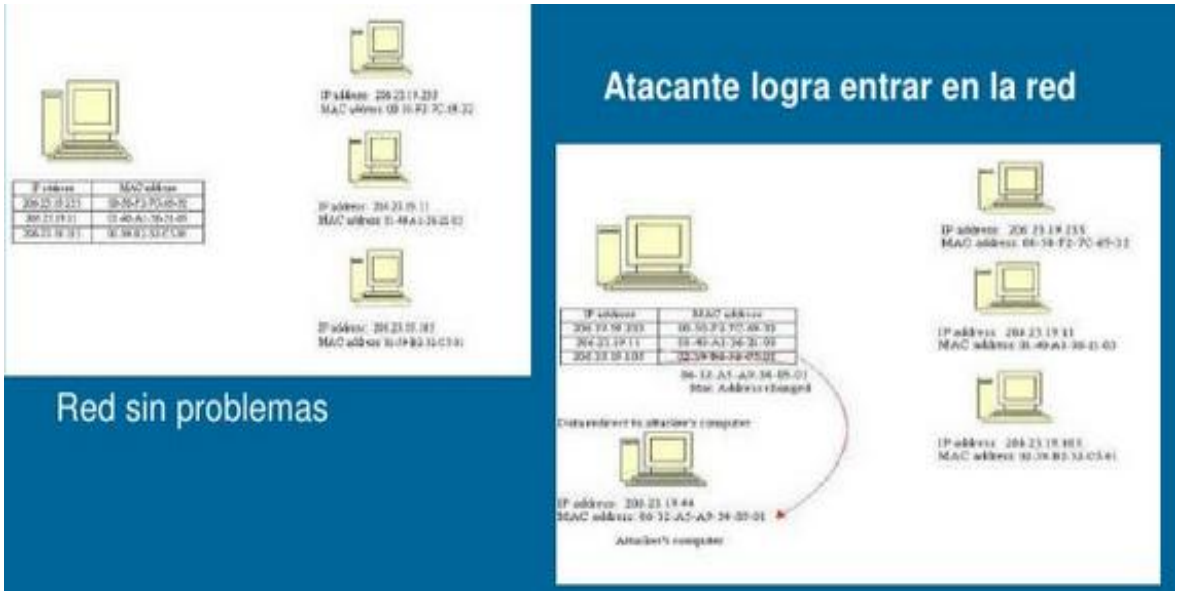


Figura 2.5.- Ataque de repetición ARP

Fuente: http://www.slideshare.net

2.1.4 ATAQUE DE REFLEXION

En este tipo de ataque el emisor recibe varios mensajes como que si fueran respuesta del mensaje que envió, pero en realidad es el mismo mensaje que envió ocasionando tráfico, logrando de esta manera cumplir sus metas.

Los ataques de reflexión se mitigan porque:

- Existe diferencia entre el orden de creación y los mensajes de dicho orden.
- Cuando el usuario envía mensajes en secuencia simplex no se reproducir debido
- Los mensajes que se dan en secuencia dúplex utilizan los ID únicos puesto que jamás se reproducirá el orden de secuencia saliente de la información como una información de secuencia de entrada.

Esquema de un ataque de reflexión

1) El intruso busca un objetivo (A) para comenzar su conexión.
2) Se produce él envió de un desafío por parte del objetivo a para confirma la autenticidad del atacante.
3) Otra conexión es abierta por parte del atacante con el receptor B, enviando el objetivo como que fuera de su propiedad.
4) Hay una respuesta al desafío por parte del receptor B.
5) Dicha respuesta es enviada por los intrusos por la conexión A donde se encuentra el objetivo A.

La respuesta es validad cuando el protocolo ha sido diñado correctamente, de otra manera la respuesta carecerá de valides, permitiéndole al intruso una conexión un canal autenticado.

2.1.5 ATAQUE DE DENEGACION DE SERVICIO (DOS)

Se trata de un ataque denominado DOS, el cual al atacar la red inhibe el acceso a un servicio, lo que hace que sea imposible utilizarlo.

Este tipo de ataque produce la caída del servicio ya que existe la perdida de la conexión de la red debido al consumo del ancho de banda.

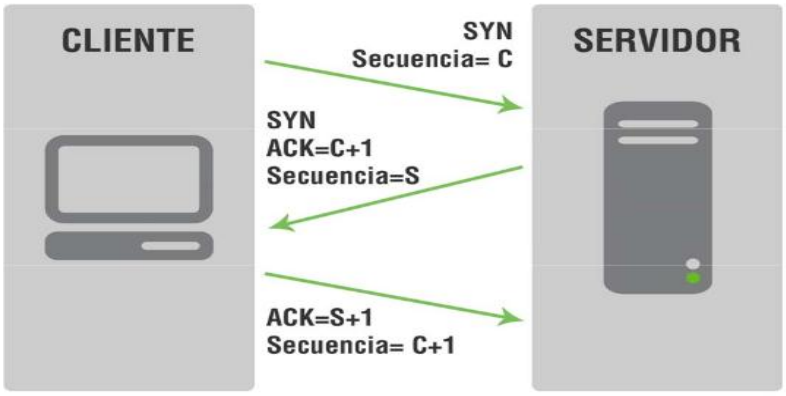


Figura 2.6.- Ataque DOS

Fuente: http://www.acens.com/

2.1.5.1 Tipos de ataques (DOS)

- **Ataque de inundación de buffer (Buffer Overflow):** es el más clásico, el objetivo es de saturar el buffer lo que obstaculiza que las peticiones las conteste el servidor de manera correcta.
- **Ataque de inundación de SYN (SYN Flood):** consiste en envíos y respuestas de mensajes, entre cliente y servidor donde se da un proceso de saludo de tres bandas; donde el usuario pide internet con un mensaje SYN al servidor , y este responde con un mensaje SYA, después el usuario envía un mensaje ACK con este mensaje se concretó la conexión.
- Pueden darse casos de saturación de tráfico por lo que el ACK se ve imposibilitado para llegar de manera inmediata, es por esta razón que durante el proceso de saludo a tres bandas, el servidor se ve obligado a mantener un tiempo de espera antes de receptar el mensaje ACK.

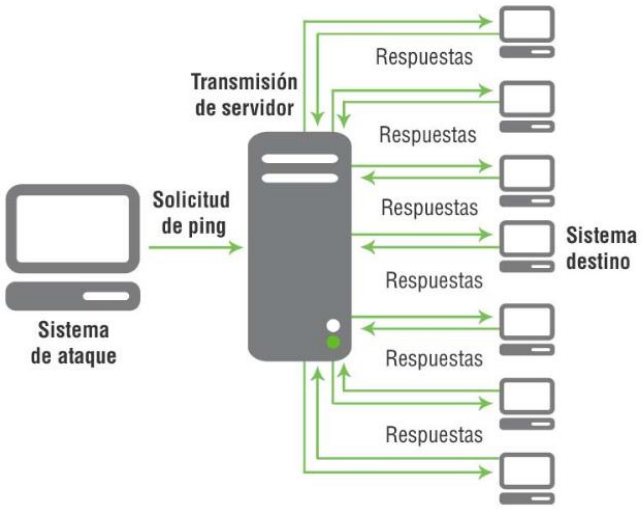


Figura 2.7.- Ataque de inundación de SYN

Fuente: http://www.acens.com/

- **Ataque Teardrop:** se aprovecha de principio de fragmentación del protocolo IP, para fragmentar grandes paquetes en pequeños fragmentos IP, cada fragmento va a tener un número de secuencia y de identificación. Por contener valores retribución puede el receptor puede volver a acoplar los datos que ha recibido.
- **Ataque de inundación ICMP:** en este ataque el sistema y la red son víctimas de una sobrecargar que impiden dar una respuesta a cierta peticiones debido a que existe una gran cantidad de petición echo reques (ping) enviadas por el atacante las mismas que son respondidas con un ICMP echo reply (pong) por par parte del servidor.
- **Ataque Smurf:** el atacante se sirve de la dirección IP para hacer él envió de paquetes ICMP echo request (ping) hacia una IP de broadcast, la victima recibirá por los demás equipos un ICMP echo reply (pong); por ejemplo si se

encuentran en una red 200 equipos y se envía un ICMP echo request (ping) haciéndose pasar por victima (Spoofing) la victima receptara 200 paquetes ICMP echo reply (pong), cuya cantidad de paquetes depende de la multiplicación ICPM inundada por el total de equipos de red.

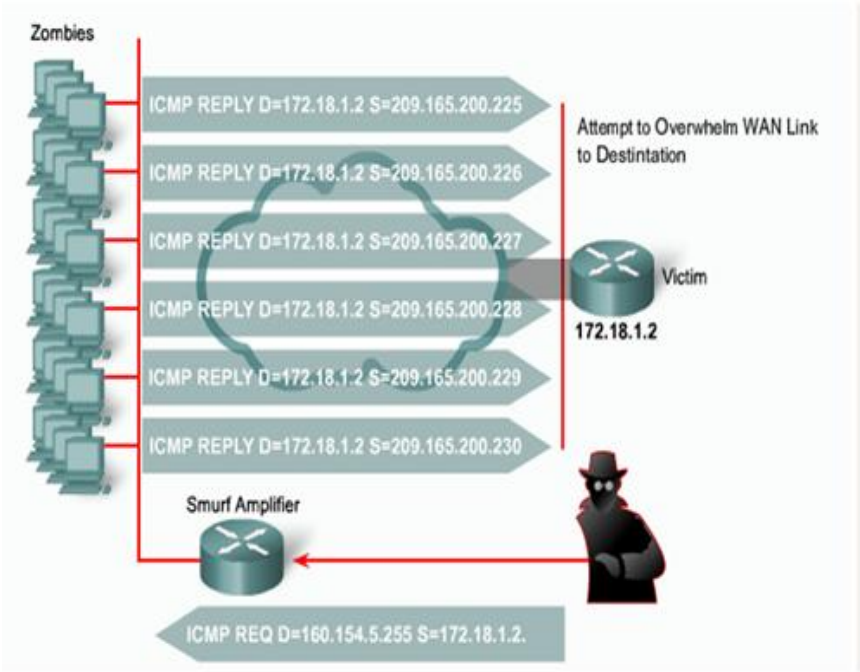


Figura 2.8.- Ataque Smurf

Fuente: http://www.cyberseguridad.net/

2.1.5.2 Clasificación de ataques de denegación de servicio

Este ataque impide que el servicio se encuentre disponible.

Tres tipos de ataques básicos:

Alberto escudero (2006) en su curso de seguridad de tipos de ataques de denegación de servicio expresa que existen tres tipos de ataques básicos:

1. Consumo de los recursos limitados o no renovables. Muy importante en el diseño de protocolos de autenticación (crypto).
2. Destrucción o alteración de la configuración de un servicio. Eg: SMTP Relay, Routing Loops.
3. Destrucción Física de los componentes.Eg. HD y sistemas de ficheros, Overclocking. (pg. 7).

2.1.5.3 Ataque de inundación de conexión

Los problemas que producen este tipo de ataque en la red, generan paquetes con origen aleatorio haciendo que el equipo de la víctima deje de funcionar.

Tipos de ataque de inundación

- **Inundación SYN:**

  Reyes Aura (2006) expresa que:

  Esta consiste en saturar el tráfico en la red haciendo uso del proceso de negociación de tres vías del protocolo tcp. Este consiste en que el cliente web realiza varias conexiones al servidor; este responde con un acuse de recibido, y el cliente web validará su conexión. En cambio suele suceder que se envían varias solicitudes con un ordenador, con información inexistente o no válida, y estos jamás reciben una respuesta de parte del servidor, provocando que este retenga conexiones abiertas en estructuras de memoria esperando respuesta, lo que puede provocar la caída del sistema si se producen muchas solicitudes (pg. 11)

- **Inundación ICMP (ICMP Flood):**

  Encontramos en este tipo de ataque un consumo exagerado en la banda ancha afecta a los equipos de computación de la víctima, ya que los sobre carga a través del envió de paquetes ICMP request o ping, los que al ser respondidos con paquetes ICMP echo replay incidirán con una sobre carga en el ancho de banda comprometiendo la capacidad del funcionamiento del servidor.

2.1.5.4 Ataque Jamming o Flooding

En este ataque la comunicación verdadera se ve afectada, por la desactiva miento de los elementos del sistema ya que el atacante satura dicho sistema por medio del envio de mensajes con direcciones IP falsas que ocasionara que las respuesta de la IP jamás sean encontradas por el sistema, el buffer se mantendrá abierto esperando que llegue la respuesta, que jamás llegaran porque direcciones fueron falsas logrando el atacante bloquear las conexiones verdaderas.

2.1.5.5 Ataque de connection flood

El número de conexiones que tiene un servidor no son ilimitadas al contrario estas tienen un límite que no puede ser sobrepasado es ahí cuando el atacante ingresa de manera intrusa ya que sin existir petición alguna establece conexiones simultaneas, Llegando a monopolizar la amplitud del servidor intentado constantemente hacer nuevas conexiones debido a que muchas de ellas se han ido caducando.

2.1.5.6 Ataque net flood

La victima en este caso se ve imposibilitada a actuar debido a que el atacante ha logrado saturar la comunicación dañando su conectividad y obstaculizando el tráfico útil.

El atacante utiliza varios puntos de red para poder enviar los paquetes de solicitud de conexión a estos se lo conoce como computadoras zombies; debido a la saturación que existe en los enlaces, las conexiones auténticas no pueden ser utilizadas.

2.1.5.7 Ataque land attack

Morocho Juan (2013) expresa que:

Este ataque consiste en un Bug (error) en la implementación de la pila TCP/IP

En sistemas Windows.

El ataque envía a algún puerto abierto de un servidor (generalmente al 113 o al

139) un paquete, maliciosamente construido con la IP y puerto origen igual que

La IP y puerto destino. Al final la máquina termina por colapsarse.

Existen ciertas variantes a este método consistente, por ejemplo, en enviar el mensaje a una dirección específica sin especificar el puerto Smurf o Broadcast Storm. Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones para a continuación mandar una petición ICMP (simulando un Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen. (pg. 51).

2.1.5.8 Ataque supernuke o winnuke

Borghello C. (2001) expresa que:

Un ataque característico, y quizás el más común, de los equipos con Windows © es el Nuke, que hace que los equipos que escuchan por el puerto NetBOIS Sobre TCP/UDP 137 a 139, quedan fuera de servicio, o disminuyan su rendimiento al enviarle paquetes UDP manipulados .(pag.56)

Actúan generalmente enviando fragmentos de paquetes Out of Band, que son detectados por parte de la víctima como inútiles lo que los coloca en un estado de inestabilidad. El termino OOB es el que normalmente debe usarse para la configuración urgente del bit.

2.1.5.9 Ataque Teardrop I y II-Newtear-Bonk- Boink

Este tipo de ataque es una verdadera amenaza por la cantidad de implementaciones que afectan directamente al IP los fragmentos no siempre se puede volver a armar de forma correcta lo que produce la caída del sistema existe muchos tipos de implantaciones las más conocidas son Newtear, Bonk Newtear, Bonk y Boink. Windows NT© 4.0 de Microsoft ® presentando vulnerabilidad de manera especial en el siguiente caso.

- **E-mail Bombing- Spamming**

Se satura el mail BOX por la frecuencia constante que con la que es enviado el mismo mensaje a una misma dirección.

Cuando el E-mail se lo envía a una cantidad exagerada de usuarios que haya o no solicitado el mensaje se está refiriendo a Spamming, el cual es muy eficaz como medio de publicidad por lo que las empresas son las que más los utilizan, aunque las leyes europeas están analizando y tratando este tipo de abuso.

2.2 FORMAS DE ATAQUE

2.2.1 PHISHING

El ataque en este caso consiste en el robo de identidad del usuario al cual el pirata informático envía un mensaje simulando ser una entidad de prestigio solicitándole a la víctima sus datos personales, para lo cual le ofrece facilidades como números telefónicos, páginas web para que la víctima caiga en su trampa y den la información personal que ellos requieren para de esta manera poder cumplir con su objetivo es decir el robo de identidad de la víctima.

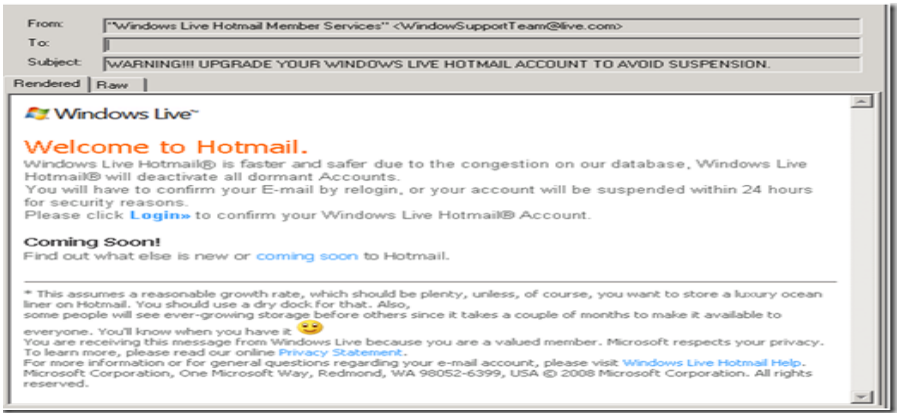


Figura 2.9.- Ejemplo del metodo de ataque Phishing

Fuente: http://www.microsoft.com/es-es/security/online-privacy/phishing-symptoms.aspx

2.2.2 SPAM

En una forma de envío masivo de mensajes para lo cual utiliza direcciones de remitentes falsas ya que el verdadero remitente oculta su identidad , las personas que se dedican a este tipo de actividad se los conocen como Spammers que buscan ganarse el dinero de una manera fraudulenta engañando a aquellos destinatarios que caen en su engaño.

2.2.3 HOAX

Se caracteriza por la distribución de mensajes de cualquier índole ya sea advertencias de salud, amenazas de virus, denuncias, casos de impacto social y espiritual etc aprovechando de la susceptibilidad, solicitándole el reenvió de dichos mensajes que algunos casos prometen algún beneficio ya sea social, espiritual o económico, con fin de que dicho mensaje sea difundido de manera masiva, aunque los hoaxes no actúan fines lucrativos si buscan atreves de estos mensajes popularidad ya que los mueve el amor propio.

Los hoaxes tienen varios objetivos entre cuales se encuentran los siguientes:

- Conseguir la mayor cantidad de direcciones de correo para enviar mensajes, spam y virus o más hoax de forma masiva.
- Uno de sus objetivos es obtener la contraseña del usuario para lo cual utiliza varias formas de engaño.
- Satura los servidores aumentado el tráfico en la red.
- Engañar a la población.
- Llegar a las redes sociales y hacerse conocido.

2.2.4 SPOOFING

Este tipo de engaño es planificado, utiliza medios electrónicos para suplantar la identidad de una persona por otra con diferentes fines que van desde la estafa hasta investigación de la vida privada de su víctima.

Para cumplir su cometido utiliza 3 máquinas, la una es para el suplantado, la otra le pertenece a la víctima y la otra que le pertenece a él.

Esta suplantación se la puede dar de diferentes maneras.

Figura 2.10.- Ataque Spoofing

Figura: http://www.slideshare.net/DaliaKarinaReyesVargas/spoofing-9548872

2.2.4.1 IP Spoofing

En este ataque la dirección del IP es suplantada con el objetivo de engañar al sistema haciéndole creer que el paquete que se está enviando lo hace desde una determinada IP.

Con el propósito de recibir la aceptación de este y recibir los correspondientes beneficios. Esto lo realiza por medio de aplicaciones especiales que han sido diseñadas, elaboradas para fines determinados se los puede utilizar en protocolos TCP/IP.

La idea es que cuando el atacante logre su misión los paquetes lleguen a la falsa IP.

Este tipo de ataque al igual que el anterior necesita de tres computadoras donde interviene el atacante la víctima y el contacto, buscando siempre suplantar el sistema para poder implementar una IP falsa, pese a todo los ángulos de los modelos de routers se convierten en un verdadero obstáculo para que este tipo de paquete no tenga acceso a paquetes con IP desconocidos o no reconocidos para las redes que son administrados con él.

2.2.4.2 ARP Spoofing

El objetivo del protocolo ARP (*Adres Resolution Protocol*) es proveer funcionalidad, asociar las direcciones MAC con direcciones IP para que de esta manera los dispositivos de la red puedan localizarse.

Para que se dé el correcto funcionamiento del protocolo ARP, las máquinas del servidor y el cliente necesitan saber la dirección MAC y además conocer si ambas máquinas están conectadas en la misma subred e incluso si es de otra red, todo esto para poder enviar un paquete entre el servidor y el cliente; además como encargado de reenviar el paquete, el cliente, requiere de una dirección MAC que es la del ROUTER.

Por medio del router, se obtendrá la dirección MAC y el cliente trasmitirá una solicitud ARP al conjunto de las máquinas que conforman la red local para detectar de quién es la dirección IP y por consiguiente quien la posea responderá con la dirección MAC.

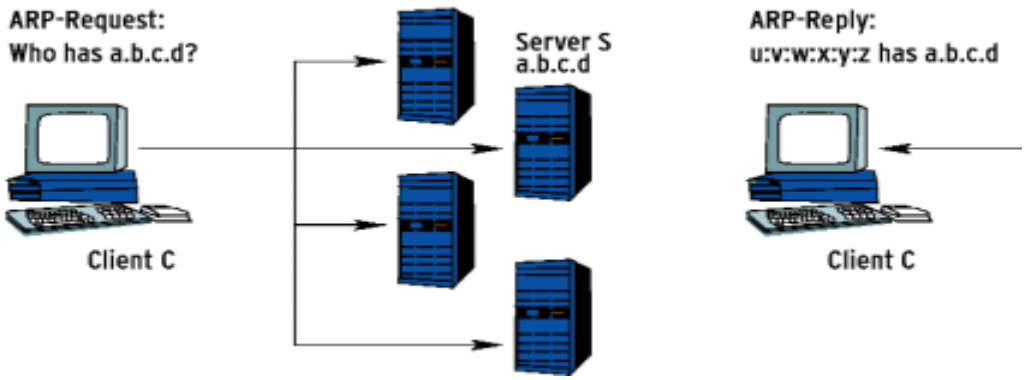


Figura 2.11. - Funcionamiento de protocolo ARP Spoofing

Fuente: http://www.linux-magazine.es/issue/09/ARPSpoofing.pdf

Con todo lo descrito en relación al protocolo ARP, se puede especificar lo correspondiente al ataque ARP *Spoofing*, el cual, es un ataque interno para infiltrarse a una red Ethernet, en donde el atacante envía mensajes ARP falsos con la finalidad de asociar las direcciones MAC con las direcciones IP de la

víctima y la muestra MAC que también está asociada, y la IP del ROUTER de la red, de esta manera todas las máquinas actualizarán sus tablas con información maliciosa, pudiendo el hombre del medio manipular las entradas del servidor cache ARP del cliente, engañando al cliente, haciéndolo pensar que la dirección MAC del atacante es la dirección del servidor, esta forma de ataque también se realiza para el servidor, como los sistemas operativos no suelen entender si su respuesta ARP es verdaderamente la respuesta a una solicitud ARP enviada previamente de la dirección de la contestación almacenada en la memoria caché, en el sistema operativo Windows, el atacante suele cambiar las entradas ejecutadas por los usuarios como estáticos, este tipo de ataque permite rebuscar los paquetes de datos que se filtran por la red LAN, modificar el tráfico o incluso detenerlo eliminando cualquier paquete recibido, permite mantener un diálogo entre el servidor y el cliente, usando la técnica del medio, los atacantes pueden dedicarse a reunir contraseñas, ya que el número de puerto les admite investigar el protocolo utilizado e identificar las credenciales del usuario, lo esencial de este tipo de ataque es aprovechar la configuración por defecto de la caché ARP, la cual se puede ver a través de la ventana de comando.

Figura 2.12.- Ventana de la Cache ARP

Fuente: http://www.expresionbinaria.com/ataque-de-tipo-arp-spoofing/

Esta cache es la que utiliza el atacante para engañar a la víctima como al Gateway que es el extremo adecuado de la comunicación y que a él se le envié su MAC lo que va destinado a la IP.

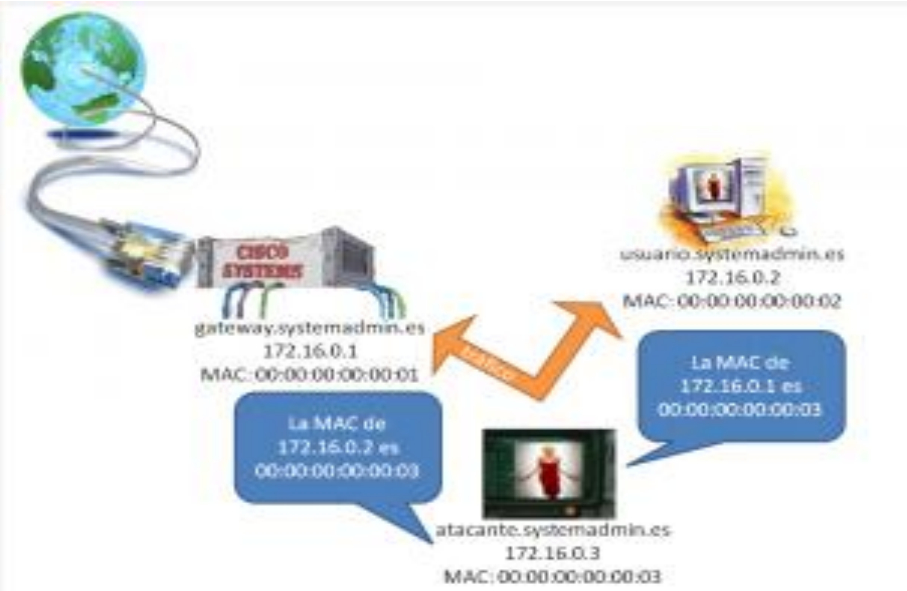


Figura 2.13.- Equipo infectado por ARP Spoofing

Fuente: http://systemadmin.es/2009/12/como-hacer-arp-spoofing

2.2.4.3 DNS Spoofing

El servidor DNS tiene la función de cambiar cada nombre de dominio (host) a cualquier dirección IP, para de esta forma poder acceder a cada máquina conectada a internet y viceversa, desde cualquier punto del mundo. El sistema de nombres de dominio en Internet es distribuido, jerárquico, replicado y tolerante a fallas. Las direcciones IP siempre están compuestas de 4 números que van desde 0 a 255 se encuentran separados por un punto.

Figura 2.14.- Servidor DNS

Fuente: http://www.uv.es/~montanan/redes/trabajos/DNS_Spoofing.pdf

Ahora, con los conocimientos previos de un servidor DNS se identificará lo que se conoce como DNS Spoofing o DNS cache poisoing/ Pharming, este ataque se particulariza por la suplantación de identidad por nombre dominio, esta anomalía es un ataque muy poderoso pero es un poco lento en relación con el ARS Spoofing.

El DNS Spoofing, cumple la función de envenenar el DNS o también puede modificar el archivo host, a esto se le da el nombre de PHARMING, provocando que cuando una persona ingrese a una página web hecha por el usuario afectado, sea automáticamente re direccionado a otra página que se encuentre bajo el dominio del atacante, llevando a la víctima a una página diferente de la que originalmente deseaba, con la finalidad de apropiarse ilícitamente de credenciales de banca en línea e información de cuenta de usuarios desprevenidos.

El DNS Spoofing ataca cuando el navegador invoca nuevamente al usuario DNS, y este a su vez transmite la petición a la red, aquí entra en juego un atacante que ve esta solicitud de petición DNS y este agresor regresa al usuario un DNS y una IP que no corresponde con la del host requerido, pero aparentemente parece que sí, de esta

forma el atacante consigue contaminar el DNS logrando modificar las entradas del servidor encargado de solucionar una cierta petición para falsear las relaciones dirección-nombre hasta comprometiendo un servidor que infecte la caché de otro, e incluso sin acceso a un servidor DNS real.

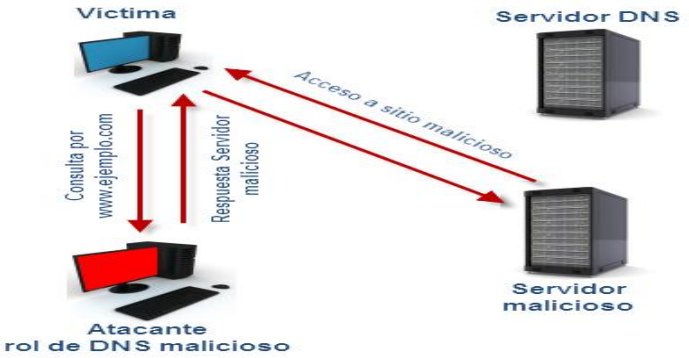


Figura 2.15. - DNS Spoofing

Fuente: http://blogs.eset-la.com/laboratorio/2012/06/18/dns-spoofing/

2.2.4.4 Web Spoofing

Este tipo de ataque es muy común y difícil de detectar, se da cuando el atacante crea un "shadow copy" de todos los portales web, el atacante dirige los accesos de estos sitios por medio de una máquina, logrando modificar o suplantar una página web real por una falsa, que aparentemente son similares, no idénticas, pero están diseñadas para apoderarse de los datos que el usuario confía en estos sitios, el hacker, a través del Web Spoofing, puede tener acceso a la visualización y posibilidades de modificación de cualquier página web que haya sido solicitada por la víctima.

El hacker puede observar y analizar el tráfico de una manera pasiva, guardando las páginas que visita la víctima y su contenido ya que el atacante controla la web irreal, es libre de modificar cualquiera de los datos que se están transmitiendo entre el servidor y la víctima en la dirección que él desee.

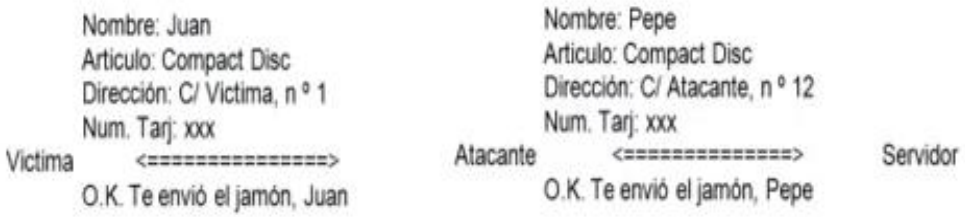


Figura 2.16.- Forma de actuar del atacante

Fuente: http://www.youtube.com/watch?v=CNZ8E2MomxI

Existe otro método que es el de instalar un software que filtra las páginas web:

1) El navegador de la víctima relaciona una página de www.atacante.org.
2) www.atacante.org se la reclama a www.servidor.com.
3) www.servidor.com se la entrega a www.atacante.org .
4) www.atacante.org recibe o modifica.
5) www.atacante.org le entrega la versión de la página que ha hecho el navegador de la víctima.

Una de las particularidades de esta forma de ataque es que también se da cuando el navegador de la víctima solicita una página con conexión segura. Si la victima ingresa a una "web segura" (usando Secure Sockets lager SSL) en un web falso, todo

sigue con normalidad, la página será mostrada, y el indicador de conexión se encenderá.

El virus web Spoofing tiene como objetivos:

- Phishing, obtener ilegalmente credenciales de otros usuarios.
- Reivindicaciones y mofa.
- Estafa

Este ataque actúa una vez que la máquina de la víctima está infectada, el hacker utiliza el código malicioso para crear una ventana del navegador, que aparentemente es inofensiva en la PC de su víctima, desde ese instante el virus encaminará todas las páginas dirigidas al equipo atacado, enviando las cargas en nuevas ventanas del navegador a través de su propio equipo, donde son modificadas para cualquier evento generado por el cliente registrado.

Es importante señalar que el virus Web Spoofing, actúa una vez que la máquina de la víctima está contaminada, desde ese momento enruta directamente al usuario que ingresa a una página real hacia una página falsa.

2.2.4.5 Mail Spoofing

Es la suplantación de identidad mediante la utilización del correo electrónico, es decir que es una técnica que se emplea para cambiar el emisor de un correo electrónico, usualmente estos e-mail se los usa para transmitir SPAM encubiertos al remitente real a través de un servidor SMTP, envía correos atribuyéndose otros nombres, cambiando las cabeceras con los siguiente textos: to , from, return- path y

reply-to, se puede detectar fácilmente que estos mensajes no se originan de remitentes reales.

Es necesario recalcar, que este virus no utiliza las cuentas para reenviarse los contactos, tampoco es un virus que parte de nuestro PC y que se expande por correo electrónico usando nuestras propias herramientas.

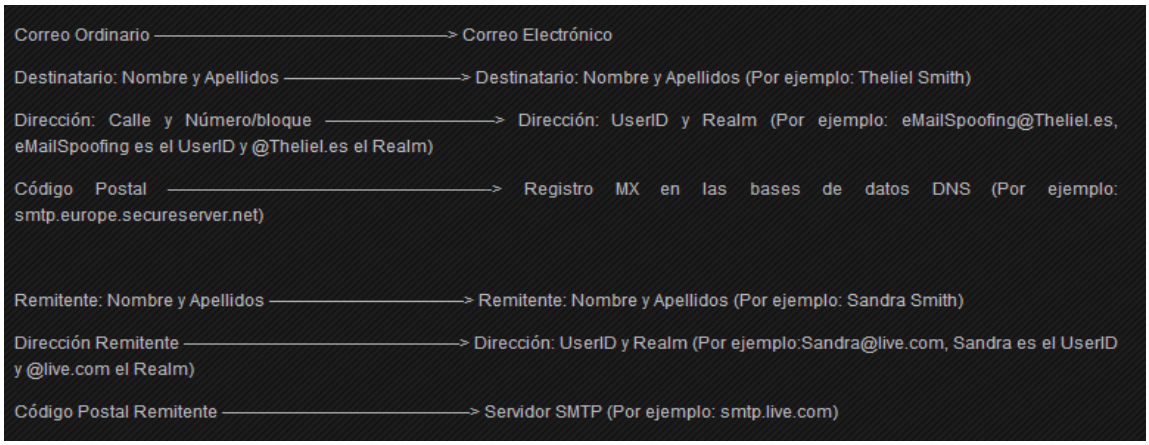


Figura 2.17. - Mail Spoofing

Fuente: http://blog.theliel.es/2010/02/seguridad-spoofing-capitulo-quinto-email-spoofing.html

Este virus, normalmente se presenta como un engaño al destinatario, para hacer una declaración de destruir la divulgación de información confidencial, como contraseña.

2.2.4.6 DHCP Spoofing

El protocolo de configuración dinámica DHCP (dynamic host configuration protocol) es una extensión del protocolo BOOTSTRAP (Bootp), el objetivo principal de la aplicación del protocolo DHCP es simplificar la administración de la

red, debido a que permite a los HOTS de una red TCP/IP obtener información de configuración básica.

FreeBSD utiliza la implementación de DHCP proporcionada por el Internet Consortium (ISC) de forma que toda la información relativa a la configuración de DHCP se basa en la distribución proporcionada por el ISC.

El protocolo DHCP principalmente se utiliza para la distribución de direcciones IP en una red, es un complemento del protocolo BOOTP, un servidor DHCP puede devolver parámetros BOOTP o la configuración específica a un determinado host.

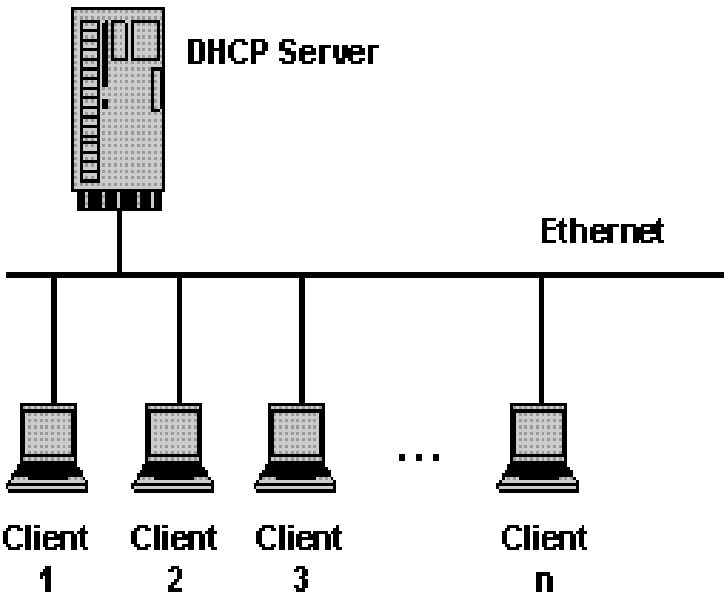


Figura 2.18. - DHCP

Fuente: http://www.monografias.com/trabajos84/servidor-dhcp/servidor-dhcp.shtml

Ahora con un conocimiento previo del protocolo DHCP, a continuación se definirá el DHCP Spoofing, el cual es un ataque a un servidor DHCP en el que el atacante intenta engañar al servidor en la obtención de la dirección IP de forma rápida y dinámica con la utilización de mensajes para obtener acceso, puede asignar default Gateway, DNS, WINS, etc. Este ataque se da envenenando la red, de esta manera las respuestas que envíe un servidor DHCP serán válidas, debido a que el hacker está en la red local, este tipo de ataque responde a consultas de clientes DHCP y también puede responder al servidor legítimo, pero si el dispositivo Spoofing está en el mismo segmento que el cliente, su respuesta al cliente puede llegar primero, ofreciendo direcciones como default Gateway o DNS erróneas.

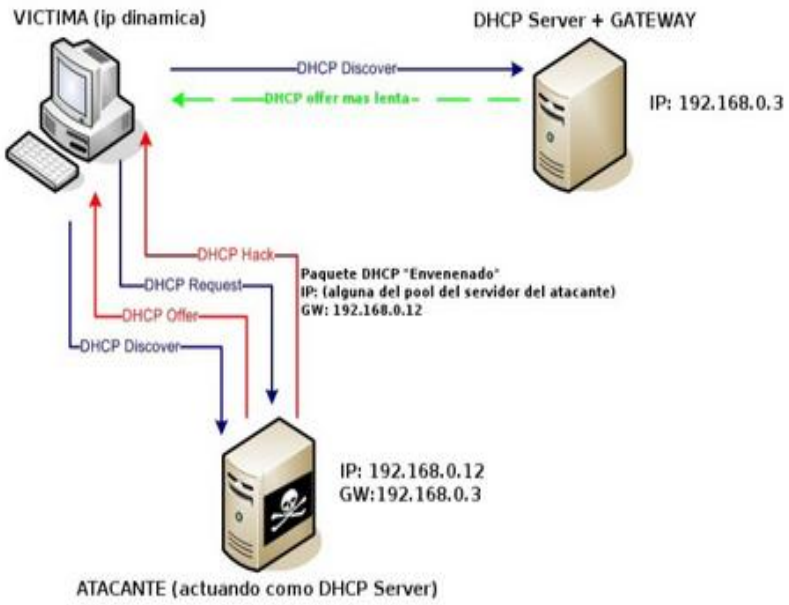


Figura 2.19. - DHCP Spoofing

Fuente: http://tic-tac.teleco.uvigo.es/profiles/blogs/ataques-a-la-capa-de-enlace-ii

El ataque se realiza cuando el usuario envía una petición de DHCP, pero el hacker ve esta petición de DHCP y responde con un falso DHCP simulando ser un servidor DHCP real, ya que está cerca del host cliente, de esta manera DNS la dirección del servidor y la dirección del Gateway predeterminado ambos estarán en dirección IP del equipo atacante, de esta forma se obtendrá toda la comunicación del host del usuario a sí mismo, y este no sabrá que su comunicación va a través del atacante.

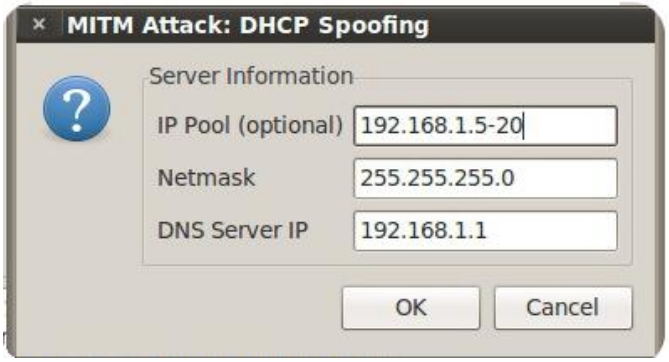


Figura 2.20.- DHCP Spoofing

Fuente: http://dtike.wordpress.com/2012/12/19/ettercap-ii-dhcp-spoofing/

El DHCP Snooping es una solución para estos ataques de "envenenamiento "o "agotamiento", son técnicas que se emplean para certificar la seguridad de una ya existente infraestructura de DHCP, una función del equipo sirve para repeler los ataques, su funcionamiento es practico solo hay que declarar al puerto al cual está conectado el DHCP corporativo (trust).

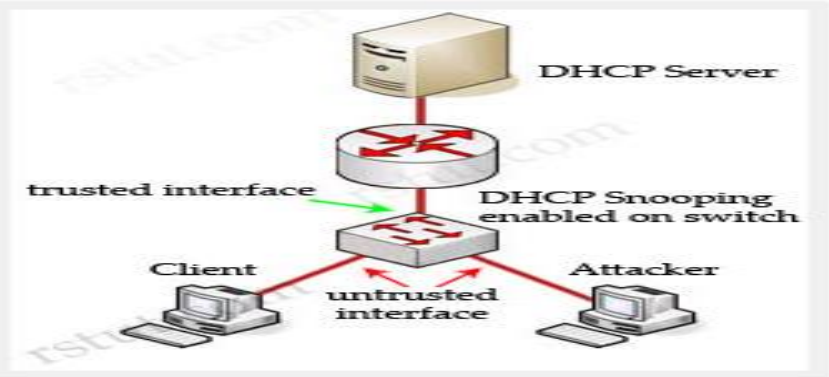


Figura 2.22. - DHCP Snooping

Fuente: http://technicafe.net/2013/05/what-is-dhcp-snooping.html

2.3TIPOS DE ATAQUE

2.3.1 ATAQUE POR INTROMISION

Este tipo de ataque se da cuando el usuario abre simultáneamente algunos archivos ordinarios, desde su equipo de computación, celulares, ipads u otra herramienta tecnológica, se da por casualidad y puede ser originado por amigos, miembros de la familia o gente externa.

2.3.2 ATAQUE DE ESPIONAJE EN LINEA

Este ataque se da comúnmente en las redes inalámbricas, puesto que en este tipo de redes no es necesario que exista un dispositivo conectado a dicha red, aquí una persona conocida o desconocida escucha e intercepta conversaciones sin ser invitada a dicho evento.

2.3.3 ATAQUE DE INTERSECCION

Es un ataque contra la confidencialidad a largo plazo, en el cual el atacante analiza los patrones a lo largo del tiempo, encargándose de desviar la información a otro punto distinto al del usuario real, para de esta forma revisar los archivos y acceder a la información deseada.

2.3.4 ATAQUE DE MODIFICACION

Por medio de este ataque, una persona no autorizada, logra cambiar o modificar a su conveniencia la información existente en un sistema, además puede cambiar los programas que se ejecutan en el sistema.

2.3.5 ATAQUE DE DENEGACION DE SERVICIO

Es un ataque a la red de computadoras, originando que sus recursos o servicios no funcionen con normalidad, para realizar esta agresión informática se necesita de muchos atacantes.

2.3.6 ATAQUE DE SUPLANTACION

Este tipo de ataque proporciona información falsa para poder negar una operación o hacerse pasar por una persona conocida. Este ataque en muchas ocasiones comienza con información obtenida de una fuente física.

La gran parte de estos atacantes usa los portales de la banca electrónica como medio para que los usuarios ingresen a sus portales falsos, atacando a la víctima por dinero, represalia o simplemente por diversión.

2.3.7 ATAQUE DE ANALISIS DE TRÁFICO

A través de este ataque, el hacker estudia el tráfico, su comportamiento, sus tipologías, debido a que los métodos utilizados para ofuscar la cantidad de datos transferidos y la encriptación no ayuda, el atacante puede decidir el remitente, el destino y el tamaño de los mensajes intercambiados.

2.3.8 ATAQUE DE MALEABILIDAD

Este ataque permite que el hacker cambie un comando FTP o el destino de una celda.

2.3.9 ATAQUE DE SYBIL

Este ataque consiste en corromper un sistema distribuido o de reputación creando una gran cantidad de usuarios falsos, todos controlados por el mismo atacante con el fin de corromper el sistema e influir en las decisiones tomadas en forma distribuida.

2.4 RECONOCIMIENTO DE UN SISTEMA OPERATIVO

El Sistema Operativo (S.O), es la parte más importante del computador, ya que, corresponde al conjunto de programas que permiten la administración eficaz de los recursos de la máquina. Cada máquina debe tener su propio S.O. que le permita realizar operaciones básicas, que van desde el reconocimiento de los dispositivos de entrada como mouse, teclado, ingresar información a la pantalla y manejar eficientemente los periféricos como escáner, impresora entre otros. Es importante remarcar que estos Sistemas Operativos en los últimos años han presentado notables cambios y contantes evoluciones.

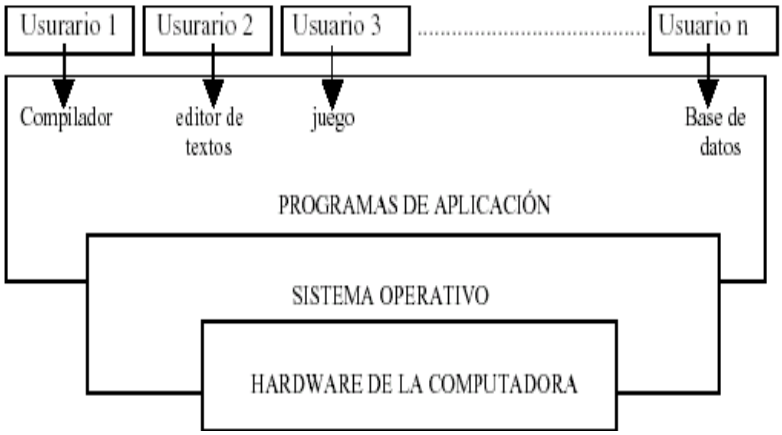


Figura 2.23.- Componentes de un S.O

Fuente: http://www.ant.org.ar/cursos/curso_intro/sistop.html

El Sistema Operativo es el encargado de crear una relación entre los recursos físicos, el usuario y las múltiples aplicaciones que están instaladas en los aparatos tecnológicos como PC, celulares, iPod, iPad, entre otros.

Funciones de un sistema Operativo

- Proporciona comodidad en el uso de computadora / usuario.
- Gestiona y fija recursos del hardware a los múltiples software.
- Gestiona y mantiene los archivos en dispositivos de memoria masiva.
- Ofrece una interfaz al usuario, ejecutando órdenes.
- Cuida los datos y los programas.
- Identifica y valida a los usuarios que utilizan el equipo de computación.
- Registra la utilización de los recursos realizada por los distintos usuarios.
- Logra que se realicen cambios sin interferir con el servicio que ya prestaban.

Las funciones de los sistemas operativos son:

- **Interfaces de usuario:** Es la parte que permite una comunicación entre el Sistema Operativo y el usuario, admitiendo que el usuario pueda descargar programas, actualizaciones y otras tareas, se basa en comandos, los que sirven para actualizar menús y las interfaces graficas de usuario.

- **Administración de recursos:** Administra los recursos de hardware, tales como: dispositivos de entrada, salida, almacenamiento, procesamiento y las redes de un sistema informático.

- **Administración de archivos:** Todo sistema posee programas de administración de archivos, los cuales se encargan de controlar la creación, borrado y acceso de archivos de datos y de programas, conserva un registro de todos los archivos que se encuentren recopilados en los periféricos de almacenamiento, discos magnéticos, etc.

- **Administración de tareas:** Esta herramienta permite controlar las actividades del sistema y su rendimiento en tiempo real, visualiza información del estado del procesador, la memoria, las aplicaciones, la red y los usuarios conectados.

Aplicaciones del Sistema Operativo:

- Muestra el estado de los programas que se ejecutan en el sistema.

- La columna “Estado” notifica si la aplicación se está ejecutando de “forma normal” cuando no hay inconvenientes en el proceso o “no responde” cuando la aplicación esta fuera de control.
- Permite finalizar, cambiar o ejecutar una nueva tarea.
- Admite cambiar una aplicación en activa que aparezca en primer plano o realizar el proceso correspondiente en el Administrador de Procesos.

En la actualidad existen diferentes tipos de S.O

2.5 TIPOS DE SISTEMAS OPERATIVOS

Sistema	Programación	Usuario único	Usuario múltiple	Tarea única	Multitarea
DOS	16 bits	X		X	
Windows3.1	16/32 bits	X			no preventivo
Windows95/98/Me	32 bits	X			cooperativo
WindowsNT/2000	32 bits		X		preventivo
WindowsXP	32/64 bits		X		preventivo
Unix / Linux	32/64 bits		X		preventivo
MAC/OS X	32 bits		X		preventivo
VMS	32 bits		X		preventivo

Figura 2.24.- Sistemas Operativos

Fuente: http://es.kioskea.net/contents/651-sistema-operativo

2.5.1 VULNERABILIDAD EN EL SISTEMA OPERATIVO

La vulnerabilidad en el sistema operativo se caracteriza por un error en la programación, implementación o configuración de un software o sistema

operativo. Se establece la diferencia entre vulnerabilidad y error, ya que la presencia de un error “normal” produce que el programa deje de funcionar y la vulnerabilidad provoca un funcionamiento “extra” del programa al permitir que este realice acciones que no ha previsto el programador, la mayoría de las vulnerabilidades de un Sistema Operativo son descubiertas y aprovechadas por un atacante.

En la actualidad se han desarrollado aplicaciones que detectan las vulnerabilidades de los sistemas y de esta manera corregirlas para poder disminuir la probabilidad de que los sistemas sean atacados con éxito, la tendencia en la actualidad es confiar en las herramientas automáticas de parcheo de los sistemas operativos y realizar un análisis de vulnerabilidades de vez en cuando para comprobar que los equipos informáticos no poseen vulnerabilidades descubiertas.

Las vulnerabilidades no solo afectan a los Sistemas Operativos, sino también al resto de aplicaciones comerciales involucradas en los procesos de negocio.

2.5.2 CONSECUENCIAS DE VULNERABILIDAD EN EL SISTEMA OPERATIVO

2.4.3.1 Robo informático

En estos tiempos, el ser humano se está volviendo dependiente de la tecnología, realizando la mayor parte de sus actividades y transacciones por internet, exponiéndose a los riesgos que conlleva la utilización del internet, puesto que esta red mundial es muy beneficiosa pero también por medio de ella se han desarrollado cosas negativas como el robo informático, esta amenaza en la seguridad informática surge por el aprovechamiento de las vulnerabilidades existentes en los sistemas, es una de las peores amenazas en la actualidad, por eso es vital proteger la información que aparece en la red y aprender a actualizar la información que se maneja.

Los robos informáticos son ocasionados por personas que tienen conocimientos avanzados en informática y telecomunicaciones, la mayoría de estos son originados por virus que están dirigidos a conseguir robo de identidades utilizando diversos objetos electrónicos para poder cumplir sus fines.

Se especifican algunas técnicas que ayudaran a evitar los robos informáticos

- Generar contraseñas alfanuméricas que sean difíciles de adivinar.
- Tener precaución con direcciones Web o URL numéricas.
- No confiar en las solicitudes de requerimiento de información básica.
- Crear copias de seguridad.

- Configurar la señal inalámbrica.
- No acceder a páginas poco confiables que no tengan certificados de garantía.

2.5.3 Modificación de mensajes transmitidos

Actualmente la mayor parte de las personas a nivel mundial se comunican a través de mensajes electrónicos, sin saber que estos mensajes pueden ser modificados, estos cambios ocurren cuando una persona sin autorización trata de reenviar mensajes y documentos que ya habían sido previamente transmitidos en el sistema de información, tras haberlos trastocados de forma maliciosa; quebrantando el modo de confidencialidad del sistema de información y privacidad de los usuarios.

Análisis de tráfico: Cada día existe un mayor número de personas que acceden a las redes y estos usuarios provocan mayor tráfico.

El análisis de tráfico es un proceso de deducir información a partir de las características del tráfico de comunicación, está basado en la tecnología Ethernet y se basa normalmente en el uso de ondas de red (software), funcionando de modo promiscuo, esta ondas detienen el tráfico que va a ser analizado y constituye la plataforma en la que se pueden ejecutar aplicaciones propietarias o de dominio público, con estas aplicaciones se puede determinar información valiosa, como: tiempo de información que circula en la red, el impacto que tiene sobre la red, de esta ,manera se puede detectar la presencia de virus, o también se puede saber si hay un excesivo uso de la aplicación

P2P (peer-to-peer o entre iguales), estas aplicaciones son aquellas que intercambian o hacen uso compartido de recursos que comúnmente degradan las aplicaciones de la red y sobre todo los enlaces principales que dan acceso a internet. En las redes modernas basadas en switches, la sonda deberá conectarse a cada conmutador.

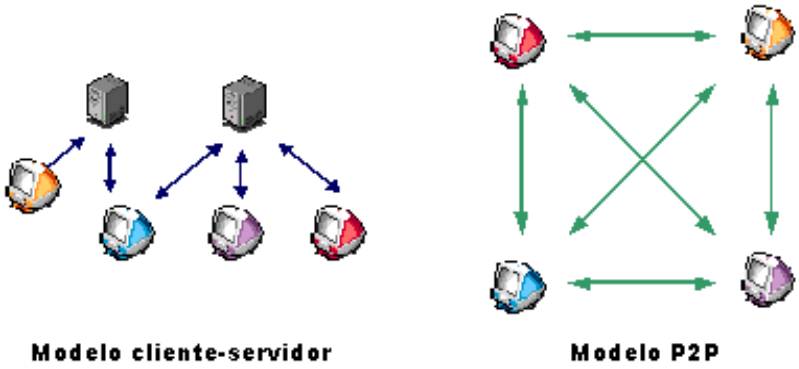


Figura 2.25.- Aplicación P2P

Fuente: http://www.internautas.org/html/3342.html

Existen diferentes maneras de realizar un análisis de tráfico, las cuales van desde productor propietarios que incluyen hardware y software, hasta soluciones gratuitas y de código abierto comúnmente utilizadas bajo el sistema operativo Linux-Unix.

Figura 2.26. - Análisis de tráfico

Fuente: http://redesrugoli.galeon.com/index11.htm

Aplicaciones gratuitas para el análisis de tráfico

Network Top (Ntop): Es una sonda de red que revela los usos de la red segregando protocolos, puertos y aplicaciones. Está basada en la librería de captura de paquetes "pcap" y bajo sistemas UNIX también se lo denomina TLP Dump.

Ethereal: Esta aplicación es un analizador de protocolos de redes muy eficaz, sus bases residen en la librería "pcap" diseñado para máquinas UNIX Y WINDOWS

La aplicación Ethereal permite capturar los datos directamente de una red o conseguir la información a partir de la captura de un disco (está en la capacidad de leer más de 20 tipos de formatos distintos). Además, se destaca por su extraordinario soporte de más de 300 protocolos.

Analyzer Colosoft Capsa 6.4 Profesional: Con la aplicación de este software, se puede examinar el seguimiento y los protocolos, captura de tráfico de una parte de la red de área local, la ventaja de este software es que puede capturar paquetes en tiempo real y analizar los datos de forma estadística.

NetworkMiner: Es un analizador pasivo de tráfico de red, al igual que Wireshark puede capturar tráfico, su principal potencial está encaminado al análisis forense del tráfico de red, es decir que Wireshark es completo y NetworkMiner es un complemento. Este analizador está basado en Windows y es Open Source, es decir es libre y no hay impedimento alguno para bajarlo y ejecutarlo en la red.

2.5 ¿QUÉ ES UNA RED CONTAMINADA O ZOMBI?

2.5.1 RESEÑA HISTORICA DE LA RED ZOMBI O CONTAMINADA

Los programas zombi en primera instancia fueron utilizados para lograr acceder a los equipos, instalar servidores, instituir recursos de cómputo y anchos de banda de manera gratuita en equipos de terceros; esta metodología se pulió de tal manera que llegó a tener programas automáticos que le permitían a los operadores de los servidores la instalación automática en diferentes equipos del mundo, con un esfuerzo mínimo.

Cuando los usuarios se enlazaron en los servidores IRC (grupos de servidores en contacto unos con otros) se extendió el número de usuarios para “chatear”, obligando a los operadores de los mismos a controlarlos y adminístralos directamente.

Esta red surge como venganza de los usuarios expulsados y se unieron para desarrollar nuevas técnicas y métodos que les permitan dañar a los servidores, en consecuencia a los canales correspondientes, ellos establecieron los ataques del tipo negación de servicio distribuido, antes de que fueran utilizados para atacar grandes empresas, esto permitió que se propagara el uso de servidores IRC para "chatear", así como su control de manera remota; con ellos se implantaron nuevas formas de utilización, a la par de servidores para enviar correo no solicitado; con ello los intrusos se percataron que podrían controlar no solo los servidores para "chatear" si no que podían hacerlo de forma remota y que para realizarlo usaban programas zombi para controlar PC, no únicamente de este tipo de servidores.

A medida que esta red surge, las empresas implementaron medidas para eliminarlos, bloquearlos y protegerse contra el uso de estos.

2.5.2 ¿QUE ES UNA RED CONTAMINADA O ZOMBI?

Las redes zombi también denominadas BOTNETS, son un conjunto de equipos en internet que se encuentran prisioneros e infectados por programas como: caballos de Troya, spyware o gusanos de propósito específico, los cuales afectan a equipos de computación desprotegidos o desactualizados en sus sistemas de seguridad, estas redes zombi son utilizadas normalmente para enviar correo no solicitado o de forma sincronizada, transmitir ataques de negación de servicio distribuido a través de la red, provocando saturación, redes pesadas, en consecuencia un impacto operacional y económico a cualquier organización.

Se calcula que existen unos 100 millones de computadores contaminados mediante virus informáticos que sirven de albergue a programas creados con tal propósito, el computador principal se filtra en el computador de su víctima y lo usa para actividades ilícitas.

El usuario normalmente desconoce que su equipo está infectado y lo puede seguir usando, aunque puede notar algunos cambios como bajas en el rendimiento del equipo.

Los atacantes con la finalidad de ampliar su alcance pueden ocultar virus de tipo troyano en archivos atractivos e interesantes en redes P2P de descarga directa gratuita.

El control del equipo de computación infectado por el programa zombi puede ser directo o indirecto:

- **Control directo:** en este caso el atacante puede establecer relación con el ordenador infectado y controlarlo utilizando las instrucciones que vienen integradas en el programa zombi.
- **Control indirecto**: en este caso el zombi se conecta por sí mismo con el centro de direcciones o con otros equipos de la red, envía una petición y ejecuta la orden o instrucción recibida como respuesta.

2.5.3 CARACTERISTICAS DE UNA RED ZOMBI

Una red Zombi tiene algunas características, las cuales dependen de la potencia que ofrece el cracker para realizar sus delitos

- **Anonimato:** El atacante actúa desde muchos ordenadores al mismo tiempo, es decir en forma simultánea, de esta forma será más difícil localizar sus ordenadores, ya que los equipos se encuentran en distintos puntos geográficos.
- **Coste:** La única inversión es el tiempo que el cracker dedica en la creación del programa, es decir es mínima, porque para las operaciones utiliza los equipos y líneas que pagan los usuarios atacados.
- **Número de equipos:** el número de equipos que forman parte del ataque es ilimitado debido a que entre más número de equipos tenga el atacante mayor será el poder que tenga en la red.
- **Actualización:** Los crackers dedican mucho tiempo para mejorar y actualizar sus programas para poder obtener más beneficios en la red.

2.5.3.1 Utilización de la red zombi

Los atacantes pueden utilizar la red zombi para dar solución a una gama amplia de inconvenientes criminales, que pueden ir desde el envío de spam hasta el ataque a redes gubernamentales.

2.5.3.2 Envió de SPAM

Es una de las maneras más fáciles y comunes de explotación de las redes-zombi, se considera que actualmente más del 80% de las cartas spam se transmiten desde redes-zombi. No son directamente dueños de la red-zombi los que remiten el spam sino que se arriendan spammers por una cómoda cantidad de dinero.

Los spammers son los que conocen el precio real de las redes-zombi. Las ganancias de un spammers fluctúan entre 50-100 mil dólares al año, miles de redes-zombi permiten a los spammers efectuar millones de envíos desde las máquinas infectadas en un espacio de tiempo relativamente corto. Las redes-zombi ofrecen a los spammers algunas ventajas a parte de la velocidad y escala de envío, como la de solucionar el problema de bloqueo de direcciones desde las que se envía spam, los spam proporcionan a la red-zombi la posibilidad de reunir en las máquinas infectadas direcciones de correo electrónico para venderlas a los spammers o para que los propios dueños de las redes-zombi envíen spam y de esta manera incrementar el número de direcciones.

2.5.3.3 El ciberchantaje

Dentro de las redes-zombi, el segundo método más popular de conseguir dinero, consiste en utilizar decenas y miles para realizar un ataque DDOT, desde las máquinas contaminadas por programas zombi se crea una serie de peticiones falsas direccionadas al servidor atacado en la red, como respuesta se da una sobrecarga y los usuarios no pueden acceder al servidor. Para frenar este ataque los crackers solicitan un rescate.

Los atacantes DDOS se utilizan también como forma de influencia política, en estas circunstancias los ataques se realizan principalmente a los funcionarios de entidades estatales o públicas.

2.5.3.4 Acceso anónimo a la red

A través de las redes-zombi, se puede lograr dinero sucio, ya que en este caso se puede dar alquiler o vender una red constituida lista para su uso. La acción de redes-zombi para su venta es una parte del negocio cibernético criminal.

2.5.3.5 Fishing

Las direcciones de las páginas de recolección de datos fácilmente pueden localizarse en las listas negras y a través de la red-zombi los "pescadores" (phishers) pueden cambiar rápidamente las direcciones de la página de recolección utilizando computadores contaminados como servidores proxy, lo que permite esconder la verdadera dirección del servidor de recolección (fisherserver).

2.5.3.4 Robo de información confidencial

Con la ayuda de las redes-zombi "Anzuelos" se pueden obtener múltiples claves para el acceso a E-mail, ICQ, recursos FTP, servidores web y otros datos secretos o privados de los usuarios. Este tipo de delito es el que atare a la mayor cantidad de atacantes cibernéticos.

Cuando el equipo está infectado, el programa atacante de la red-zombi puede descargar automáticamente otro programa dañino, en el caso de los virus troyanos

dirigidos a robar contraseñas, toda la red se contaminará y se permitirá a los atacantes el robo masivo de claves de acceso o contraseñas.

Las contraseñas sustraídas se comercializan o se utilizan para realizar infecciones masivas de páginas web, con la finalidad de extender posteriormente el programa zombi dañino y de esta manera ampliar la red-zombi.

2.5.3.5 Órdenes que cumplen las redes Zombi

Las órdenes que cumplen los programas zombi son muy variadas y se detallan a continuación:

- **Update:** Es una orden básica y es la que debe cumplirse en primera instancia, y si el propietario de la red-zombi quiere instalar una nueva versión del programa zombi (bot), esta orden permite renovar el archivo zombi ejecutable siguiendo la instrucción de su dueño. Esta orden permite contaminar al computador con programas dañinos, tales como virus, gusanos, así como facilita la instalación de programas troyanos simultáneamente en todos los ordenadores, estos virus troyanos investigan todas las contraseñas que hayan sido ingresadas en algún momento en el ordenador y almacenadas en su memoria, y luego los transmite al servidor en internet.
- **Flood:** Se crea un conjunto de solicitudes falsas direccionadas a un servidor específico de internet con el fin de que el servidor deje de trabajar o de sobrecargar el canal de internet del segmento indicado en la red global.

  La creación de este tipo de flujos puede ocasionar graves desajustes en el servidor que impedirán el acceso a los usuarios simples.

- **Spam:** Se carga el patrón de mensaje spam y se comienza a enviar spam a las direcciones seleccionadas, cada red-zombi tiene una proporción de direcciones.
- **Proxy:** La función del servidor proxy casi siempre está incluida en la función del programa zombi (bot), es una de las funciones que permite utilizar cualquier computador de la red-zombi como servidor proxy con la finalidad de esconder la dirección verdadera del cracker que dirige la red-zombi, estas órdenes suplementarias permiten lograr duplicados de las pantallas del usuario, controlar las teclas que se pulsan en el teclado, pedir archivos del protocolo de la red de comunicación del usuario (se usa para robar cuentas y datas confidenciales) reenviar el archivo indicado desde el computador del usuario, pedir la lista de ordenadores que conforman parte de la red zombi, etc.

2.5.4TIPOS DE RED ZOMBI

Las redes zombi se clasifican según su arquitectura y protocolos usados en la dirección de programas zombi.

2.5.4.1 Clasificación de redes-zombi según su arquitectura

Redes-zombi con un centro único.- las redes-zombi con esta arquitectura o todos los ordenadores-zombi se conectan con un único centro de dirección C&C (Comand & Control Centre; Centro de dirección y Control). El C&C espera la conexión de nuevos programas zombi; los incluye en sus base, cuida su estado y les da órdenes, que son seleccionadas por el propietario de la red-zombi del listado de posibles órdenes para programas (bots). Todos los programas zombi se ven unos a otros en el C&C y para manejar la red necesitan el acceso de control y dirección.

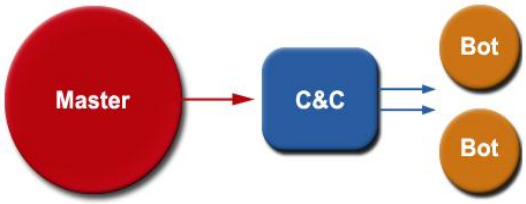


Figura 2.27.- Topología Centralizada (C&C)

Fuente: http://www.viruslist.com/sp/viruses/analysis?pubid=207270986

Las redes-zombi de control centralizado son el tipo de red zombi más divulgado, porque es fácil crearlo, controlarlo y tiene reacción más rápido a las instrucciones, combatir con redes-zombi centralizadas también es más sencillo, para neutralizar esta red-zombi es suficiente cerrar el C&C.

Redes-zombi descentralizadas o P2P.- redes zombi – (del inglés “peer-to-peer”, que significa conexión del tipo “punto-punto”). En caso de una red-zombi descentralizada, los zombis no se vinculan con el centro de control, sino con algunas máquinas contaminadas de la red-zombi, las instrucciones se envían de un programa zombi a otro: cada zombi posee un detalle de direcciones de algunos “vecinos” y al recibir la orden de uno de ellos, transmite esta orden a los demás.

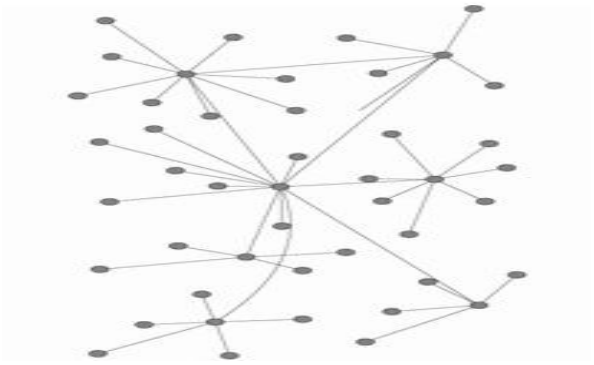


Figura 2.28.- Topología Descentralizada

Fuente: http://entropia.blog.br/2011/05/05/os-perigos-da-recentralizacao-do-mundo-de-pontas/

El diseño de una red-zombi descentralizada en la práctica no es muy cómodo, dado que se necesita proporcionar a cada computador infectado la lista de aquellos programas zombi (bots9) con los que se relacionan en la red-zombi. Esta topología mixta también corresponde al tipo P2P, a pesar de que en cierto momento se use C&C. Combatir con este tipo de rede-zombi es más complicado porque en la red-zombi activa no existe un centro de control.

2.5.4.2 Clasificación de redes-zombi según el uso de protocolo de red

Para propagar el programa zombi el propietario de la red-zombi, necesita como mínimo instalar una conexión de red entre el ordenador-zombi y el ordenador del que parten las instrucciones. Todas las interacciones de red están fundadas en los protocolos de red que delimitan las reglas de comunicación de los computadores dentro de la red, por eso existe una clasificación de redes-zombi basada en el uso de protocolos de comunicación. Se clasifican en:

- **Las de orientación IRC.-** Fue una de las primeras redes-zombi, en la cual el control de zombis se hacía usando IRC (Internet Relay Chat, es decir, charla interactiva internet). Cada ordenador contaminado se enlaza con el servidor IRC indicado en el cuerpo programa-zombi, entraba en un canal determinado y esperaba las órdenes de su propietario.
- **Las de orientación IM.** Este tipo de red-zombi no es muy popular. Se diferencia de los de orientación IRC únicamente en que para la transmisión de datos se utilizan canales IM (Instant Messaging) es decir, canales de servicio de mensajería instantánea como: AOL, MSN, ICQ y otros. La escasa fama de estas redes-zombi se debe a los problemas que aparecen al crear una cuenta separada de servicio IM para cada programa zombi (bot). La situación es que los programas zombi deben salir a internet y estar constantemente en línea. En vista de que la mayoría de los servicios IM no permiten entrar en el sistema desde diferentes computadores utilizando una misma cuenta, cada programa zombi debe tener su propio número de servicio IM. Además los propietarios de servidores de mensajería instantánea imposibilitan de diferentes formas cualquier registro automático de cuentas. Como resultado los dueños de orientación IM están muy limitados en cuanto a número de cuentas registradas, y por ende en el número de zombis que estén activos en la red. Los zombis pueden usar la misma cuenta para estar en línea cada cierto tiempo, enviar los datos al número del propietario y durante un corto tiempo esperar la respuesta. Este tipo de red tiene una reacción muy lenta a las órdenes.
- **Las de orientación web.** Este tipo de redes-zombi son populares porque son muy fáciles de diseñar, debido a que existe una gran cantidad de servidores

web en internet y porque son sencillos de controlar a través de una interfaz web. Esta es una rama relativamente de redes-zombi vigiladas a través de www. El zombi se conecta con un determinado servidor web, recepta de este las instrucciones y envía los datos como respuesta.

- **Otros.** Además de los descritos anteriormente, hay otros tipos de redes-zombi, que se comunican en base a su propio protocolo basándose únicamente en la estructura o stack TCP/IP: utilizan solo protocolos generales TCP, ICMP, UDP.

2.5.5 FASES DE LOS EQUIPOS INFECTADOS

1) **Desarrollo**: Es la primera fase al momento de crear una Botnet. En este caso el cracker determina la manera de trabajar del software malicioso y de la red.
2) **Fase de infección:** es la segunda parte, comienza cuando se infecta el primer ordenador y continúa mientras el software malicioso no sea detectado y detenido por los antivirus, y de esa manera logra propagarse a otras máquinas.
3) **Explotación:** En esta fase la red contaminada lleva a cabo sus actividades para las cuales fue diseñada.
4) **Declive:** Esta fase es cuando se reduce el número de equipos infectados, provocando que la operación deseada no funcione.
5) **Inactividad:** Es cuando la red deja de funcionar.
6) **Modificación:** En esta fase el cracker realiza cambios en el software malicioso para que realice otras funciones, evitan su detención o aumentar la velocidad de expansión.

2.5.5.1 DEFENSA CONTRA UN ATQUE ZOMBI

Lamentablemente no existe un sistema de protección al 100%, por eso es imperante tomar las medidas necesarias como, asegurarse de contar con la versión actualizada de antivirus en el ordenador, la administración del antivirus el cual consiste en actualizarse de las crecientes definiciones de virus, gusanos y códigos maliciosos.

La protección más eficaz para impedir que el cracker obtenga el control de los ordenadores de una red consiste en unificar un sistema de detención de zombis rápido y eficaz en las soluciones de seguridad de punto y de Gateway.

Hacer uso de las denominadas paredes de fuego, ya que, por medio de los firewall se restringe el acceso no autorizado al equipo que está conectado a internet. No abrir archivos adjuntos que provengan de contactos no conocidos o no deseados.

Cambiar constantemente las contraseñas de los emails, cuentas bancarias y demás sitios web. Desconectarse de internet cuando no se lo esté utilizando. No ingresar a enlaces sospechosos o peligrosos.

2.5.5.2 ¿CÓMO CONTAMINAN LOS ATACANTES UNA RED Y CUÁL ES SU FINALIDAD?

La red se infecta a través de un virus que no es ningún tipo de programa, el virus únicamente produce daños a las redes, es manipulado por un atacante o cracker.

Para que el cracker pueda infectar la red necesita de que el usuario ejecute su código por lo menos una vez. Este código es ejecutado de manera involuntaria, es decir, sin

que el usuario se percate cuando abra páginas de la web, archivos, correos o programas que estén infectados con un virus malicioso. Estos virus pueden se pueden presentar de cualquier forma; en discos prestados, en discos que se puedan adquirir en una tienda o simplemente al descargar de internet una página web o un servidor FTP, mediante el intercambio de archivos (P2P) o como adjunto de un mensaje de correo.

Los atacantes utilizan diferentes mecanismos para realizar la inyección de su virus.

- **Vulnerabilidades de los sistemas operativos:** Por lo general los atacantes o crackers se aprovechan de las debilidades que posee un sistema operativo para poder realizar sus ataques, estas debilidades son fallas, errores que tiene un sistema operativo convirtiéndolo en un blanco fácil para cualquier ataque.
- **Páginas web:** Hoy en día la gran mayoría de las páginas web y las redes sociales tienen virus, el cual se puede contraer simplemente con visitar cualquier página web infectada.
- **Ejecutables "camuflados":** Algunos virus están escondidos o camuflados en archivos de datos que tienen nombres raros, falseando su extensión o utilizando íconos de archivos populares que resulte conocido por el usuario.
- **Ingeniería social:** Normalmente redactan mensajes que llamativos para atraer la atención del usuario, logrando de esta forma persuadir a los usuarios inexpertos y ejecuten programas o páginas maliciosas.

El atacante infecta la red con muchos propósitos, los cuales dependen del malhechor, algunos lo hacen para ganar fama y ser reconocidos, para robar cuentas bancarias,

para obtener información privada, definitivamente en la mayoría de los casos para cometer actos delictivos.

2.6 ¿QUÉ SE PUEDE HACER CON UNA RED CONTAMINADA?

Con una red infectada se pueden producir diferentes tipos de ataque, tener una red contaminada suele ser un excelente negocio, puesto que se puede robar a entidades bancarias números de cuentas a fin de cometer diferentes tipos de actos ilícitos.

2.6.1ROBO DE INDENTIDAD

Con todos los problemas morales, sociales y económicos por lo que está atravesando la sociedad, actualmente nos encontramos totalmente expuestos a un robo de identidad. Las estadísticas reflejan que México y España encabezan la lista de países que sufren en gran escala por este tipo de fraude o estafa.

Normalmente los phishers (suplantación de identidad) buscan en la red servidores web con debilidades que puedan ser usados para montar páginas que intenten suplantar la identidad de una institución financiera de tal forma que el usuario no pueda notarlo. Para la victima tiene como repercusión la afectación directa en su servidor de internet, ya que la IP clon se encuentra alojada en la página del fraude.

Como funciona: El atacante envía múltiples mensajes falsos que aparentemente provienen de instituciones de prestigio como entidades bancarias, estos mensajes se los remite a varias personas. Algunos crackers logran engañar a las personas que

creen que los mensajes son verdaderos y dan respuesta a sus pedidos proporcionándole datos personales como el número de cuenta de tarjeta de crédito.

Para que estos mensajes parezcan reales el atacante puede incluir link falsos que direccionan a los usuarios a un sitio web aparentemente legítimo, pero que en realidad es un sitio falso o incluso puede re direccionar a una página emergente que aparentemente tiene el aspecto de una página real.

Estas copias se las conoce como "sitios web piratas" y una vez que el atacante obtenga los datos, este puede fingir ser la víctima.

Como protegerse de un robo de identidad: Este tipo de fraude debe contraerse a través del ISP y la víctima.

- Jamás se debe responder a solicitudes de información personal a través de correo electrónico. Si se tiene dudas es preferible comunicarse con dicha entidad. Tener cuidado con correos que supuestamente han sido enviados por entidades financieras y compras por internet como Ebay, PAYPAL, bancos, etc…
- Asegurarse si el ordenador cuenta con las últimas actualizaciones a nivel de seguridad dadas por el fabricante (Microsoft, MAC, etc.).
- Para visitar un portal Web, introduzca la dirección URL en la barra de direcciones.
- Asegurarse que el sitio web utiliza cifrado.

- Si tiene instalado un servidor web, asegurarse que tanto el aplicativo como el sistema operativo cuenten con las últimas actualizaciones a nivel de seguridad dadas por los fabricantes correspondientes.

Principales daños que causa el robo de identidad:

- Perjuicios económicos para los usuarios de las redes corporativas (ancho de banda, saturación de correo etc.)
- Pérdida de productividad.
- Consumo de recurso de las redes corporativa

Una de las modalidades de *phishing* es el *pharnming*. Es una técnica que consiste en cambiar el sistema de resolución de nombres de dominio (DNS) para direccionar al usuario de una página falsa.

Cuando el usuario ingresa una dirección en su navegador, esta debe ser convertida a una dirección IP numérica. Este proceso es lo que se denomina reducción de nombres, y de esto se encargan los servidores DNS.

Existen ejemplares de malware diseñados para modificar el sistema de resolución de nombres local, ubicado en un fichero denominado HOSTS.

Este fichero permite guardar de forma local esa resolución de nombres asociados a direcciones IP. De esta manera aunque el usuario introduzca en el navegador el nombre de una página web legítima, el ordenador primero debe consultar al fichero HOSTS si existe una dirección IP asociada a ese nombre. En caso de no encontrarla, lo consultará con el servidor DNS de su proveedor.

2.6.2 MODIFICACION DEL TRÁFICO Y TABLAS DE ENRUTAMIENTO

Consiste en desviar del destino los paquetes de datos de su ruta original a través de internet, para enviar la información por redes, equipos intermedios o dispositivos intermedios antes de llegar a su destino original, de esta manera facilita las actividades de intercepción de datos.

Mecanismos para llevar a cabo este tipo de ataques:

- **Utilización del encaminamiento fuente ("*source routing*"):** esta funcionalidad está disponible en el protocolo IP y admite que el cracker especifique una determinada ruta prefijada, la que se emplea como ruta de retorno, saltándose todas las reglas de ruteo definidas en los ruteadores de la red.

  De esta manera utilizando además el "IP Spoofing", un atacante podrá hacer pasar cualquier máquina en el que el destino pueda confiar, para recibir a continuación los datos correspondientes al equipo suplantado.
- **Utilización de paquetes de control del tráfico:** es una funcionalidad disponible en el protocolo ICMP mediante el paquete "ICMP Redirect" que permite cambiar la ruta en un destino específico.
- **Modificación de las tablas de ruteo:** mediante la utilización de protocolos de ruteo dinámico, como RIP o BGP.

  Al modificar las rutas, el tráfico atravesará equipo y redes antes de alcanzar su destino final, facilitando el "Snifing".

2.6 TIPOS DE INTRUSOS O ATACANTES

En la actualidad existen personas que se dedican a realizar actividades ilegales y actividades en favor de la humanidad por medio del internet a estas personas se las conoce como Hacker y Cracker.

2.6.1 HACKER

El término Hacker surgió en los años 80 por un grupo de ingenieros físicos que formaban parte del MIT (Instituto de Tegnologia de Massachusstts), cuyos programadores se auto denominaban “Hackers” debido a que eran los responsables de hacer “hacks” (alteraciones) de programas en sus antediluvianas TX-O se convirtieron en los “hackers” del equipo.

La palabra inglesa hackers quiere decir divertirse con el ingenio, es decir usar la inteligencia para hacer algo difícil. Son programadores apasionados por la seguridad informática, manejan perfectamente la informática y la electrónica para poder comprender sistemas muy complejos, la mayoría de los hackers actúa por el deseo de obtener más conocimiento y el reto de desafiar el funcionamiento de los ordenadores y servidores de internet, muchas personas piensan que los hackers son los autores de virus, de robos de identidad y de algunos eventos ilegales, pero realmente eso es un error, puesto que los verdaderos hackers contribuyen en el mejoramiento de la seguridad de internet, una persona se aparte de la definición de hacker cuando usa sus conocimientos con fines dañinos y realiza actividades malintencionadas convirtiéndose en un “craker”.

El objetivo de un hacker es saltar los sistemas de seguridad de internet para llegar una vez adentro no causa ningún daño; una vez que el hacker logró evadir la seguridad deja una "bandera" que es una señal de que logro romper la seguridad y encontró la vulnerabilidad, para que el administrador mejore los niveles de seguridad.

2.6.2 CRACKERS

El término Crackers se deriva de la palabra Hacker y surgió en 1985 como contraposición al término Hacker, con la diferencia que el Cracker realiza actividades fuera del marco de la ley. La palabra inglesa cracker "romper" se utiliza para aquellas personas tienen la capacidad der romper los sistemas de seguridad y software.

En algunas situaciones el cracking es la única forma de hacer actualizaciones de software para el que su fabricante no presta soporte en el momento que se precise hacer actualizaciones, corregir errores, únicamente en estos casos no se considera al cracking como una actividad ilegal.

Los Crackers son el grupo más rebelde de expertos en informática, ya que a más de romper la protección de seguridad en un sistema, hace pública esta acción difundiéndolo en la red para conocimiento de otras personas.

Los crackers modernos usan software propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web, tales pasos para desbloquear claves de acceso o generadores de números para que en forma aleatoria y ejecutados automáticamente puedan lograr violar claves de acceso de los sistemas.

En la actualidad es común ver internet cracks de algún software de forma gratuita a través de internet.

2.6.3 WANNABES

Es la etapa inicial de un hacker, un wannabe adquiere el estatus de hacker cuando los veteranos resuelven comenzar a considerarlo como uno de los suyos.

2.6.4 PHREAKERS

El movimiento Phreak inicia con la invasión del teléfono por Alexander Graham Bell en 1876, quien pensó que sería utilizado para que la gente escuchara música, sin embargo esta idea no funcionó y como consecuencia tuvo la brillante idea de dar libertad a las personas para que estas hicieron lo que se les ocurra con esto.

Es una de las más antiguas prácticas en la historia del cibercrimen, la cual inicia en 1971 cuando un veterano de la guerra de Vietnam, John Draper conocido como "Capitán Crunch*",* descubrió como un silbato podía reproducir el tono de 2600 hertz de los sistemas telefónicos.

Phreaker o Cracker de las redes de comunicación, son aquellas personas que tienen amplios conocimientos de la telefonía, son apasionados del sistema telefónico, investigadores de las telecomunicaciones, ya que, con sus amplios conocimientos pueden llegar a estafar a las empresas de telecomunicaciones para que estas no cobren las llamadas, esta actividad se la denomina Phreaking, también pueden realizar llamadas sin que el propietario de la línea se dé cuenta que desde su teléfono se está realizando una llamada.

Enfoque

Dirigen sus estudios y ocio hacia el aprendizaje y comprensión del funcionamiento de teléfonos de diferentes características.

Tecnologías de telecomunicaciones.

Funcionamiento de empresas telefónicas.

- Sistemas que componen una red telefónica.
- Electrónica aplicada a sistemas telefónicos.

El propósito de los Phreaker es obtener llamadas gratuitas, realizar espionajes, o solo destrozar la seguridad de las líneas. Son personas muy buscadas por la justicia sobre todo debido a la presión de las grandes empresas de telecomunicaciones.

2.6.5 LAMERS

Es una persona que no tiene conocimientos y tampoco la intención de adquirirlos aunque presume de ellos.

El Lamer usualmente utiliza programas creados por crackers y presume de sus "logros", con la ayuda de estos software pretende robar claves de correos electrónicos o acceder a ordenadores de forma no autorizada, son los responsables de propagar virus y bombas lógicas en la red con la única finalidad de fastidiar y que otros se enteren que usa tal o cual programa. Son novatos que presumen de lo que no son.

2.6.6 SAMURAI

Es una persona contratada para averiguar las debilidades que tiene un sistema de seguridad, indaga casos de delitos informáticos usualmente relacionados con la violación de derecho de privacidad. Los samurái están en contra de cualquier vandalismo electrónico, se basan en leyes que permiten sus acciones, además se dedican a realizar nuevos sistemas de seguridad y conocer sobre la seguridad con sistemas en redes.

2.6.7 PHISHER

Son aquellas personas que pretenden conseguir información confidencial por un medio que supuestamente es genuino, de esta manera la víctima no podrá fácilmente darse cuenta de que es engañada. Los phisher son los que diseñan páginas web de bancos, gestores de correos electrónicos, compañías de prestigio, de este modo que al ponerse en contacto con la victima esta acceda a la página falsa, y se registre enviando información confidencial a una página web falsa.

2.6.8 SCRIPT KIDDIE

Denominados Skid Kiddie o Script kiddie, se trata de múltiples usuarios de internet, sin conocimiento sobre hack o el crack en su puro estado, son inexpertos en los sistemas informáticos que interrumpen dichos sistemas con la aplicación de herramientas automatizadas pre-empaquetadas y diseñadas por otros.

Se dedican a buscar software de hacking en la red y después los ejecutan sin leer los ficheros Readme de cada aplicación, transmitiendo virus y de esta forma destruyendo sus propios ordenadores.

Generalmente usan cracks, exploits como WinNuke, Back orifice, Netbus y software parecidos diseñados por personas con conocimientos, la razón por la cual realizan estos actos es presumir ante conocidos y amigos.

2.6.9 MOTIVOS DE LOS ATAQUES A REDES

Existen muchos motivos que pueden tener los atacantes.

- Atracción a lo illegal.
- El deseo de conseguir dinero.
- El deseo de ganar fama y tener reconocimiento de las amistades
- El deseo de hacerse perjuicio.
- Esto puede ser ejecutado por empleados internos que abusan de sus autorizaciones de acceso, o por atacantes externos que acceden vagamente o obstruyen el tráfico de red.

2.6.1 Procedimientos que usan los atacantes

Algunos de los pasos que utilizan los atacantes para lograr acceder a un sistema son los siguientes:

- Reconocimiento pasivo.
- Reconocimiento activo (Escaneo-Scanning).

- Explotando el Sistem (Exploiting).
    - Logrando Acceso a través de:
        - Ataques al Sistema Operativo.
        - Ataques a la Aplicaciones.
        - Ataques por medio de pequeños programas (Scripts).
        - Ataques a la configuración del sistema.
    - Elevación de Privilegios.
    - Denegación de Servicios (Denial of Service).
- Subir programas.
- Descargar datos.
    - Conservar el Acceso usando:
        - Puertas Traseras (Backdoor)
        - Caballos de Troya (Troyan Horse)
- Cubriendo el rastro.

Reconocimiento Pasivo: Para poder vulnerar un sistema el atacante debe tener información sobre lo que va a atacar y que va hacer. El reconocimiento pasivo puede brindar toda la información que el atacante precisa para acceder, con el reconocimiento pasivo el atacante puede establecer sus debilidades más notorias, aparentemente el reconocimiento pasivo no es tan útil, pero no se debe subestimar la cantidad de información que el atacante puede adquirir si lo hace adecuadamente.

El reconocimiento pasivo permite que:

- No se haga ningún tipo de escaneo o contacto con el equipo de computación objetivo.

- Construir un mapa del objetivo, sin interactuar con él.
- Existan menos herramientas informáticas que en las otras fases.
- La Recolección de Información Pública (Internet, Ingeniería Social y Google Hacking).

Reconocimiento Activo: Corresponde a la segunda etapa, y consiste en la identificación activa de objetivos, mediante el escaneo de puertos, y las identificaciones de servicios y sistemas operativos.

- Identificar Estado de Puertos.
- Identificar Servicios
- Identificar Sistema operativo.
- Existe contacto directo con el Objetivo.
- Banner Grabbing "Captura de Banners"

Explotando el Sistema: La gente cree que explotar el sistema únicamente es lograr un acceso, pero actualmente se trabaja en dos áreas adicionales que son: la elevación de privilegios y la denegación de servicios.

El cracker puede usar un sistema de una Red para atacar a otra red. Por ejemplo: El agresor puede utilizar los ordenadores de la compañía X, para acceder a los ordenadores de la compañía Y, cuando la compañía y realice las investigaciones todo indicará que la compañía X es la culpable. A este tipo de problemas se los conoce con el nombre de Downstream Liability el cual puede tener aplicaciones legales para una entidad, si la encargada del cargo de seguridad informática no realizó las actualizaciones en cuestiones de seguridad.

Adquiriendo Acceso: Es una de las maneras más notorias de explotar un sistema, existen muchas formas con las que un atacante puede acceder a un sistema, pero en el nivel más importante el atacante debe aprovechar al máximo un determinado aspecto de una entidad. El cracker usualmente detecta las vulnerabilidades físicas de la seguridad o las debilidades en la construcción de sistemas. La clave es reducir al mínimo esas debilidades para proporcionar un ambiente seguro.

A continuación, se detallan algunas maneras de cómo un atacante puede acceder a un sistema:

- Ataques al Sistema Operativo.
- Ataques a las Aplicaciones.
- Ataques por medio de Pequeños Programas (Scripts).
- Ataques a la Configuración del Sistema.

    - **Ataques al sistema Operativo:** Los ataques a los sistemas Operativos se los realiza cuando encuentran errores en ellos, las fallas en un sistema operativo deja muchos servicios corriendo y puertos abiertos y de esto se aprovechan los atacantes para poder infectar al sistema operativo.
    - **Ataques a las aplicaciones:** Los ataques a las aplicaciones se aprovechan de la poca seguridad que tiene a nivel lógico del software. El tiempo de desarrollo de programación para muchas aplicaciones es muy corto y no tiene en cuenta su seguridad. Uno de los problemas del software que se está desarrollando es el tiempo que tienen los programadores y los probadores ya que tienen mucho trabajo, debido a

este problema la prueba en algunos casos no las completan como se debería. La seguridad no debe estar en agregar o parchar componentes, debe tener un nivel de seguridad desde el momento que diseñaron dicha aplicación para no tener complicaciones en el futuro.

- **Ataques a la configuración del sistema:** La mayoría de los casos en que un sistema tiene problemas, se debe a que no fueron configurados correctamente. Son muchos administradores que instalan un sistema con las opciones por defecto o por otra parte al tratar de instalar un nuevo programa modifica una serie de opciones hasta que logra que un producto trabaje, el problema con esto es que el nunca deshace lo que hizo o limpia el trabajo extraño realizado, y esta es la razón por la que algunos sistemas son violados y otros no.
- **Elevación de privilegios:** Esto se da al suministrar permisos de autorización a un cracker más allá de los concedidos inicialmente. Por ejemplo, un atacante con un conjunto de privilegios de permisos de "solo lectura" eleva de algún modo el conjunto para incluir la "lectura y escritura".
- **Denegación de servicios (Denial of Service):** Los dos tipos de ataques primordiales son negación del servicio y ruptura interna. La negación del servicio es un ataque a un sistema o red que tiene como propósito la denegación del servicio, es decir, que el sistema o red no pueda servir normalmente las peticiones a usuarios genuinos. En un DOS se genera una enorme cantidad de peticiones desde un host en particular, lo cual satura los servicios que corren de cara al servidor y generalmente

provoca la pérdida de conectividad de la red por un alto consumo de ancho de banda, o una sobrecarga por un alto número de paquetes por segundo (ppts). Son ataques son fáciles de realizarse en Internet debido a que no se requiere ningún acceso anterior, al estar conectados a internet nos volvemos vulnerables a un ataque de Denegación de Servicio.

Subir programas: Para que un atacante pueda acceder a un sistema la víctima tuvo que ejecutar una descarga o cargar un archivo o programas del sistema, porque si no el atacante tardaría mucho tiempo para poder acceder al sistema de la víctima. Cuando el atacante indaga para hurtar información, después de que tenga acceso, su meta será descargar la información lo más secretamente posible y luego salir del sistema. En la mayoría de los casos, el atacante instalará programas en el sistema para poder tener más privilegios, acceder con mayor facilidad y convertirlo en una plataforma de trabajo.

Descargar datos: Normalmente en los ataques para realizar espionaje corporativo, al atacante únicamente le importa la información, en estos casos el atacante desea el acceso ilegal al sitio para luego hacer un traspaso de los datos a otras partes, después de que la información sea descargada el efectuará un análisis sobre dicha información.

Conservado el acceso: Después que el atacante ingresa al sistema, él puede colocar una puerta trasera para poder acceder cuando él lo desee, en la mayoría de los casos el atacante conserva accesos a ese sistema para utilizar esos ordenadores como plataforma para lanzar ataques con otras entidades. Una puerta trasera puede ser tan fácil como agregar una nueva cuenta de usuario al sistema, es sencillo pero si la

compañía verifica sus cuentas activas, puede descubrirla, es más difícil de detectarla con millones de cuentas. Un tipo más sofisticado de puerta trasera es la de sobrescribir un archivo del sistema con una versión que tenga una particularidad oculta, esto permitirá que el usuario no se dé cuenta de que sistema está comprometido, a estos programas modificados que están instalados son conocidos como Caballos de Troya porque tienen una característica oculta. Otra forma que tiene el atacante para crear una puerta trasera es instalar un programa servidor sobre cualquier máquina de un usuario, para que cuando el atacante se conecte a dicho programa pueda tener acceso completo al sistema o aún más a la red.

Cubriendo el rastro: Cuando el atacante haya cumplido su misión, este debe asegurarse de no ser atrapado por eso cubre sus huellas. Los más fácil es limpiar los registros del sistema que se crean diariamente, estos archivos contienen un expediente que indica que personas accedieron al sistema y cuando de esta manera cualquier persona que visualice el contenido de los logs puede detectar fácilmente que persona no autorizada ingreso al sistema y determinar también el trabajo que realizo sobre la máquina. Por eso el atacante lo primero que hace es descubrir donde se encuentran los logs del sistema y luego limpia dentro de los archivos los registros que se relacionan con su ataque. Hay dos desventajas importantes para realizar esta acción.

1) Al ver que el contenido de los logs han sido eliminados levantaría sospechas inmediatamente de que algo está ocurriendo.

2) Cuando un sistema está bien instalado y administrado puede lanzar una advertencia al administrador de que uno o varios archivos logs del sistema fueron modificados en sus tamaños o indicar que el archivo se borró.

Por esta manera se recomienda recolectar los logs del sistema en una máquina alterna o emitirlos directamente a un medio de impresión. De esta manera las oportunidades de que alguien busque los logs del sistema y los limpie se reducen al mínimo. Otra técnica del atacante es suspender los registros sobre los logs del sistema tan pronto como él acceda al sistema, de esta manera no tendrá que borrar ningún registro y nadie sabrá lo que ha hecho.

CAPÍTULO III SEGURIDAD EN LA RED

3.1 ¿QUÉ ES SEGURIDAD EN LA RED?

En la actualidad se considera al internet como un medio de comunicación y colaboración, se estima que alrededor de 57 millones de usuarios de internet han sufrido algún tipo de ataque a la red debido a las pocas e ineficientes de medidas de seguridad en un problema tan grave y que está creciendo.

La seguridad en redes es mantener bajo protección información, recursos con que se cuenta en la red, a través de procedimientos basados en una política de seguridad que avalen la seguridad tanto física como lógica de la información.

Sin ningún tipo de seguridad la red se encontraría expuesta ante cualquier atentado, ocasionando intromisiones no autorizadas, periodos de inactividad de red, interrupción del servicio, incumplimiento de las normativas e incluso de las acciones legales.

La seguridad no solo tiene un método, sino que utiliza un conjunto de barreras que defiende a la compañía de diferentes maneras, inclusive si falla una de las soluciones, se conservarán otras para proteger a la empresa y cualquier información.

Una buena seguridad de red nos ayuda a:

- Evitar que algunas personas no autorizadas intervengan en el sistema con fines perversos.
- Evitar que los usuarios realicen operaciones inconscientes que puedan perjudicar el sistema.

- Asegurar los datos mediante la prevención de fallas.
- Avalar que no se interrumpan los servicios.

3.1.1 LAS CAUSAS DE INSEGURIDAD

- **Un estado de inseguridad activo,** la falta de conocimiento del usuario acerca de las funciones del sistema, algunas de las cuales pueden perjudicar al sistema.
- **Un estado de inseguridad,** cuando el usuario o administrador no está habituado con el mecanismo de seguridad en el sistema.

3.1.2 COMO UTILIZAN LAS EMPRESAS LAS TECNOLOGIAS DE SEGURIDAD

La seguridad de red es importante debido a que la mayoría de empresas se encuentran expuestas a cualquier tipo de ataque informático. Sus clientes, proveedores y partners comerciales seguramente esperan que proteja toda la información que comparten.

Confianza de los clientes:

- Privacidad garantizada
- Fomento de la colaboración

Una buena seguridad garantizará que cualquier información que tengan los clientes en la empresa estará a salvo de cualquier tipo de ataque. Sus partners tendrán mayor

confianza de compartir información, ayudándole a colaborar y trabajar conjuntamente de una forma más eficiente.

Movilidad

- Existirá un acceso completamente seguro fuera de la oficina.
- Fomento de la productividad fuera de la oficina.

Una seguridad de red fuerte, ayuda a permitir que los empleados puedan acceder de forma segura a la red desde fuera de la empresa sin tener miedo de que un virus pueda infectar o cualquier otro tipo de amenaza.

Los empleados podrán tener acceso a información importante cuando la necesiten y de esta manera aumentará la productividad cuando no se encuentren en la oficina.

Productividad mejorada

- Poco tiempo dado al Spam
- Mejor predisposición y colaboración de los empleados.

Los empleados dedicarían menos tiempo a actividades no productivas, como la recepción de spam o enfrentarse a virus, y ocuparán ese tiempo en el trabajo.

Reducción de costos

Si se tienen un buen nivel de seguridad se evitara pérdidas económicas ya que al existir problemas en la red pueden existir periodos largos de inactividad, una seguridad efectiva ayudara a poder emplear nuevas aplicaciones, crear nuevas

aplicaciones sin dañar el funcionamiento de red para que de esta manera la compañía no genere pérdidas y pueda seguir creciendo.

3.1.3 PLANIFICACION DE LA SEGURIDAD EN REDES

Es necesario de una planificación de la seguridad de redes para evitar perjuicios posteriores y trabajos para que la red se encuentre en óptimas condiciones.

La falta de una planificación puede acarrear problemas como:

- Que personas no autorizadas ingresen en el sistema.
- Perjuicios intencionados o no intencionados.

Niveles de seguridad de red:

Universidad de Alcalá (2007) considera que:

Dependiendo del grado de "sensibilidad" de la información personal contenida en cada fichero, se definen distintos niveles de seguridad, englobando cada uno al anterior como si se tratara de un sistema de capas concéntricas donde la más alta contiene a la inferior.

Cada uno de estos niveles se corresponde con la exigencia de determinadas medidas de seguridad que debe cumplir el responsable del fichero.

Por tanto, la legislación establece tres niveles de seguridad**:**

• **Básico:** aplicable a todos los ficheros que contengan datos de carácter personal.

• **Medio:** para todos los ficheros que traten datos de carácter personal y contengan información sobre infracciones administrativas o penales, o para cualquier fichero que contenga un conjunto de datos que permita definir o evaluar la personalidad de un individuo. Por ejemplo, les correspondería a este nivel los ficheros que contengan sanciones administrativas impuestas a alumnos o al personal de cualquier Universidad.

Asimismo, aunque no es aplicable en el ámbito de las Universidades, los ficheros cuyos responsables sean las Administraciones Tributarias en el ejercicio de sus potestades tributarias, o aquellos cuyos responsables sean las Entidades Gestoras o la Seguridad Social para fines recaudatorios, etc.

• **Alto:** aplicable a los ficheros que traten datos de carácter personal y contengan información sobre ideología, religión, creencias, afiliación sindical, origen racial, salud, vida sexual, o con fines policiales. Por ejemplo, el fichero Actividades Deportivas podría incluir información sobre religión (derivada de la selección o no de una determinada actividad deportiva), salud (minusvalías u otras circunstancias de salud que supongan la necesidad de actuaciones específicas), etc. El Reglamento incluye en este nivel los que contengan datos derivados de violencia de género. Se establecen excepciones en la asignación del nivel alto en función de la finalidad, permitiendo aplicar el nivel básico en los casos recogidos en el Artículo 81 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de 15/1999.

3.1.4 AUTENTICACION MEDIANTE NOMBRE DE USUARIO Y CONTRASEÑA

En este método debería ser suficiente para empresas pequeñas y personas comunes que no requieran de altos niveles de seguridad ya que es un método básico para proteger la información de la red IP.

3.2 ¿CÓMO DEFENDERSE DE UN ATAQUE A LA RED?

Los atacantes se basan en los fallos de diseño, en protocolos y en los sistemas operativos utilizados.

Ante cada tipo de ataque la solución debe ser inmediata, mantenerse informado y de todas actualizaciones que se den.

Una de las tácticas para defenderse es:

1. Se debe acceder al panel de control del enrutador por medio de internet y cambiar la contraseña en el panel de inicio y el nombre del usuario.
2. Modificar u esconder el nombre identificador del conjunto de servicio (SSID).
3. Atreves del protocolo dinámico de host (DHCP) cambiar el rango de las direcciones IP dadas por el enrutador.
4. En el enrutador habilitar el control de acceso a medios (MAC).

3.3 MEDIDAS DE SEGURIDAD QUE SE DEBEN TOMAR

Medidas preventivas que se deben tomar:

1) Mantener al día las maquinas con sus actualizaciones debidas y físicamente seguras.
2) Tener personal especializado en seguridad informática.
3) A pesar de que la información que contenga el PC no pueda parecer valiosa, al atacante le puede parecer útil en el momento de emplear el ataque DOS.
4) No permitir el tráfico "broadcast" desde fuera de nuestra red. De esta forma evitamos ser empleados como "multiplicadores" durante un ataque Smurf.
5) Introducir el tráfico IP Spoof
6) Filtrar el tráfico IP Spoof.
7) Realizar auditorías de seguridad y sistemas de detección.
8) Es recomendable estar informado sobre las debilidades que se encuentran en nuestro sistema y parches lanzados.

CAPITULO IV CONCLUCIONES Y RECOMENDACIONES

Después del estudio, finalmente se pueden plantear las conclusiones a las que se llegó con la investigación y exponer las recomendaciones permitentes.

4.1. CONCLUCIONES

- De acuerdo al análisis de resultados, un monitoreo e identificación a ataque a redes permite tener una red contralada y evitara problemas red.
- El monitoreo pasivo puede realizarse a través de distintas técnicas, las cuales pueden acompañarse de la definición de métricas o alarmas garantizando así el buen funcionamiento de los dispositivos de red.
- Cualquier tipo de vulnerabilidad que tenga el software, sistema operativo u otro tipo de vulnerabilidad será aprovechado por personas con intenciones maliciosas.
- Tener un buen sistema de seguridad en la red puede ayudar a tener la información bajo protección.
- Se cumple el objetivo de Caracterizar e investigar los elementos que intervienen en la seguridad en redes para mejorar la misma mediante instrumentos y protocolos de seguridad, de acuerdo a la necesidad de los usuarios que requieren mejor protección y privacidad de la información que circula en su red.

4.2 RECOMENDACIONES

- Conocer el alcance los dispositivos que van hacer monitoreados.
- Tener las actualizaciones de los antivirus.
- Conocer las nuevas formas de infección a la red.
- Tener una planificación de seguridad en la red.

Referencias Bibliográficas

- **BIBLIOGRAFIA DE LIBROS**

- Dordoige y Atelin. Redes. (2006).*Informáticas conceptos fundamentales normas, arquitectura, modelos OSI, TCP/IP, Ethernet, Wi-fi (Edición Original)*. Cornella de Llobregat (Barcelona).
- Universidad Nacional Autónoma de México. (2005). *Monitoreo de recursos de red*. México: Altamirano Carlos.
- Universidad Tecnologica Nacional Regional Santa Fe.(2010.). *Seguridad en la red principios de la seguridad en los sistemas de información ataques a la seguridad de la información Servicios y mecanismos de seguridad*.: Cesar Ballardini.
- Arango, Jhon. (2010). *El atacante informatico*.: IT Forensic Ltda.
- Alonso, J., Guzman, A., Laguna, P y Martin, A. (s.f.). *Ataques a aplicaciones* Web.: Universidad Oberta de Catalunya.
- Universidad de Alicante. (2010). *Redes y transmisión de datos*: Gil. P., Pomares. J y Candelas. F.
- Universidad técnica particular de Loja. (s.f.). M*onitoreo de la red* .Loja.: Abarca, N., Cruz, P., Palacios, G y Sarmiento, Cisne.
- IES Gregorio Prieto. (s.f.). S*eguridad y alta disponibilidad .:* Madrid Nicolás.

- **BIBLIOGRAFIA DE TESIS Y MONOGRAFIAS**

  - Carnegie Mellon University (2001). *Amenazas lógicas*. EE.UU: Borghello Cristian.
  - Universidad Tecnológica Equinoccial (2003). *Aplicación de Software que permita detectar y neutralizar intrusos a nivel de la capa de aplicación, en el modelo de referencia TCP/IP*: Recalde y Salas.
  - Universidad de San Carlos de Guatemala (2012). *Aseguramiento y seguridad en servidores web caso de estudio. Guatemala*.: Aura Cifuentes.
  - Universidad Autónoma del estado de Hidalgo. (2008). *El hacking y técnicas de contra-ataques a la seguridad de información*. Pachuca-México: Ponce María
  - Universidad Autónoma del estado de Hidalgo. (2005). *Redes de transmisión de datos.:* López Vicente
  - Escuela superior politécnica de Chimborazo. (2009). *Estudio de las técnicas de análisis de flujos IP y su aplicación en el monitoreo de redes de datos en la escuela de ingeniería en sistemas perteneciente a la FIE.* Riobamba.: Castro, A. y Estrella, A.
  - Universidad Nacional de Colombia. (2006). *IPMONITOR Y CACTI.* Bogotá.: Adelaida, A.
  - Universidad de las Palmas de Gran Canaria. (2006). *Tutorial de NT-SNMP*. *Hernández, L.*

- Escuela Politécnica Nacional. (2013). *Implementación de un firewall sobre plataforma Linux en la empresa de contabilidad armas & asociado.* Quito.: Morocho Juan.

- **ARTICULOS DE INTERNET**

- *Conceptos Generales sobre redes LAN. (s.f.).* Recuperado el 4 octubre del 2013, dehttp://infoplc.net/files/documentacion/comunicaciones/infoplc_net_ConceptosSobreRedes.pdf
- *Martinez Evelio (2007).* Redes LAN, CAN, MAN Y WAN; Tipos de redes basadas en la distancias de cobertura. Recuperado el 3 de noviembre del 2013, del sitio web del Eveliux: http://www.eveliux.com/mx/redes-lan-can-man-y-wan.php
- *Definición de LAN, MAN Y WAN. (2012).*Recuperado el 3 de noviembre del 2013, de http://bioelectrinik.blogspot.com/2012/02/definicion-de-lan.html
- *Quinodoz Carolina (2009).* Conceptos de Redes LAN: Recuperado el 3 de noviembre del 2013, del sitio web del Blog de Informática, Educación Tecnologica y Tics: http://profecarolinaquinodoz.com/principal/?p=370
- *Definición de Red. (s.f.).* Recuperado el 4 de noviembre del 2013, de http://www.mastermagazine.info/termino/6496.php
- *Red informática. (2006).* Recuperado el 4 de noviembre del 2013, de
- http://www.larevistainformatica.com/red-informatica.htm

- *Redes MAN, Redes WAN. (s.f.*). Recuperado el 4 de noviembre del 2013, de http://www.unicrom.com/
- *Ferrer, N., Salas M., Belisario, M., Blanco, D. y Piñango C. (2008*). Recuperado el 4 de noviembre del 2013, de http://aprendaredmanunerg.blogspot.com/
- *The State University of New Jersey. (1988, septiembre).* Introducción a la Administración de una Red Local. Recuperado el 5 de noviembre del 2013, del sitio web de Computer Science Facilities Group: http://es.tldp.org/Manuales-LuCAS/doc-red-local-inet/doc-red-local-inet-html/
- *Asociación Red Universitaria de Alta Velocidad del Valle del Cauca. (2012).* ¿Qué es una red académica de Tegnologia avanzada?. Recuperado el 4 de noviembre del 2013, del sitio web de : http://www.ruav.edu.co/index.php/quienes-somos/que-es-una-raav
- *Red de área metropolitana (MAN). (2014*). Recuperado el 4 de noviembre del 2013, de http://www.ecured.cu/index.php/Red_de_%C3%81rea_Metropolitana
- *Web Spoofing con PHP. (2011).* Recuperado el 5 de noviembre del 2013, de http://www.aztlan-hack.org/index.php?command=1003&noticia=Web-spoofing-basico-con-PHP
- *Web Spoofing (2010).* Recuperado el 4 de noviembre del 2013, de http://blog.theliel.es/2010/02/seguridad-spoofing-capitulo-tercero-web-spoofing.html

- *¿Qué es el Spoofing? (1901*). Recuperado el 5 de noviembre del 2013, de http://www.zonavirus.com/articulos/que-es-el-spoofing.asp
- *Martin David. (2010*). Recuperado el 5 de noviembre del 2013, de
- http://www.redeszone.net/2010/10/30/web-spoofing-suplantacion-de-una-web-con-la-finalidad-de-recoger-los-datos-introducidos-por-el-usuario/
- *Guash J. (2013).* Recuperado el 6 de Noviembre del 2013, de http://www.securitybydefault.com/2013/07/zarp-framework-para-ataques-de-red.html
- *Ataques de denegación de servicio (DOS) (Ataques Informáticos III). (s.f.).* Recuperado el 6 de noviembre, de http://www.cyberseguridad.net/index.php/197-ataques-de-denegacion-de-servicio-dos-ataques-informaticos-iii
- *Universidad de Alcalá. (s.f.).* Ataques de Denegación de Servicio. Recuperado el 6 de noviembre del 2013, del sitio http://it.aut.uah.es/enrique/docencia/ii/seguridad/documentos/t11-0506.pdf
- *Escudero P. (2006).*Curso de Seguridad Tipos de ataques de denegación de servicio. Recuperado el 7 de noviembre del 2013, de http://www.it46.se/courses/security/materials/es/01_Intro_Security/es_security_B1C_dosattacks_slides_escuderoa.pdf
- *González Ramón. (2013).* Recuperado el 7 de noviembre del 2013, del sitio de http://ramon-gzz.blogspot.com/2013/02/ataque-dos-inundacion-syn.html

- *Reyes, P. L. (2012).* Seguridad, defensa digital. ¿Qué es y cómo funciona un ataque DDOS?. Recuperado el 8 de noviembre del 2013, de http://revista.seguridad.unam.mx/numero-12/que-es-y-como-funciona-un-ataque-ddos
- *Tipos de ataque. (2014).* Recuperado el 6 de diciembre del 2013, de http://www.vilecha.com/Seguridad/tipatak.asp
- *Reconozca correos electrónicos de suplantación de identidad (phishing) o vínculos de este tipo. (s.f.).* Recuperado el 7 de diciembre del 2013, de http://www.microsoft.com/es-es/security/online-privacy/phishing-symptoms.aspx
- *Spam ¿Qué es exactamente?.(s.f.).* Recuperado el 7 de diciembre del 2013, de http://www.viruslist.com/sp/spam/info?chapter=153350526
- *Scam, Hoax, Phishing, Pharming, Ransomware e Ingenieria Social. (s.f.).* Recuperado el 7 de diciembre del 2013, de http://www.gitsinformatica.com/scam.html
- *Federación Argentina de Cardiología. (2010).* Virus, Hoax y Spam. Recuperado el 7 de diciembre del 2013, del sitio web de: http://www.fac.org.ar/1/ayuda/virspan.php
- *¿Qué es un Hoax?. (2007).* Recuperado el 8 de diciembre del 2013 , del sitio web de Que sepan : http://paraquesepan.blogspot.com/2007/04/qu-es-un-hoax.html
- *Fain Alejandro. (s.f.).* Recuperado el 7 de diciembre del 2013, de http://www.pablofain.com/que-es-un-hoax

- *Pocalles J. (2004).* Recuperado el 7 de diciembre del 2013, de http://winred.com/internet/que-es-un-hoax/gmx-niv113-con2260.htm
- *Demuth, T. y Leitner, A. (s.f.).* Recuperado el 7 de diciembre del 2013, de http://www.linux-magazine.es/issue/09/ARPSpoofing.pdf
- *Ataque de tipo ARP Spoofing. (2013).* Recuperado el 7 de diciembre del 2013, de http://www.expresionbinaria.com/ataque-de-tipo-arp-spoofing/
- Arp Spoofing. (2010). Recuperado el 7 de diciembre del 2013, de http://www.cristianamicelli.com.ar/?p=494
- *DNS Spoof or Split-Horizon DNS "How to". (2013).* Recuperado el 7 de diciembre del 2013, de https://calomel.org/dns_spoof.html
- *Catoira F. (2012).*Recuperado el 7 de diciembre del 2013, de http://blogs.eset-la.com/laboratorio/2012/06/18/dns-spoofing/
- *Mail Spofing: Mails con falso remitente, que si son devultos por no encontrar destinario, se devuelven al que figura como remitente, causando extrañeza al usuario en cuestión. (2013).* Recuperado el 7 de diciembre del 2013, de http://www.zonavirus.com/noticias/2013/mail-spoofing-mails-con-falso-remitente-que-si-son-devueltos-por-no-encontrar-al-destinatario-se-devuelven-al-que-figura-como-remitente-causando-extraneza-al-usuario-en-cuestion.asp
- *Hablemos de Spoofing. (2010).* Recuperado el 7 de diciembre del 2013, de http://hacking-etico.com/2010/08/26/hablemos-de-spoofing/
- *Sánchez, C. (2013).* Experts en actacs controlats a Sistemes Informatics.: Ataques al servicio DHCP (II): DHCP Spoofing con Ettercap Hacking

Etic. Recuperado el 7 de diciembre del 2013, del sitio Web del Hacking Etic: http://www.hacking-etic.cat/?p=932&lang=es

- Cesar. (2010). Recuperado el 7 de diciembre del 2013, de http://tic-tac.teleco.uvigo.es/profiles/blogs/ataques-a-la-capa-de-enlace-ii
- *DHCP Snooping. (s.f.).* Recuperado el 8 de diciembre del 2013, de http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/snoodhcp.html
- *Prevent DHCP Server Spoofing by using DHCP Snooping. (2012*). Recuperado el 8 de diciembre del 2013, de http://howdoesinternetwork.com/2012/prevent-dhcp-server-spoofing
- McNamara Michael. (2013). Recuperado el 8 de diciembre del 2013, de http://blog.michaelfmcnamara.com/2013/01/dhcp-snooping-arp-inspection-ip-source-guard/
- *Astorino,J. (2011).* Recuperado el 8 de diciembre del 2013, de http://astorinonetworks.com/2011/06/28/going-deep-with-dhcp-snooping/
- *Asgar,A. (2013).* Recuperado el 8 de diciembre del 2013, de http://technicafe.net/2013/05/what-is-dhcp-snooping.html
- *Sutter, G. (s.f.).* Recuperado el 8 de diciembre del 2013, de http://www.freebsd.org/doc/es/books/handbook/network-dhcp.html
- *Elie. (2010).* Recuperado el 9 de diciembre del 2013, de http://redeselie.blogspot.com/2010/06/tipos-de-ataques-ataque-por-intromision.html
- *Ataqus comunes. (2010).* Recuperado el 8 de diciembre del 2013, de http://redescebolla.wordpress.com/tag/interseccion/

- *López, J. (s.f.).* Recuperado el 8 de diciembre del 2013, de http://es.scribd.com/doc/19397003/Tipos-de-Ataques-informaticos
- *Gonzalez, MaPilar. (s.f.).* Recuperado el 8 de diciembre del 2013, de http://platea.pntic.mec.es/vgonzale/pc_10/archivos/_124/Tema_2.1.htm
- *Vulnerabilidad. Seguridad Informatica. (s.f.).* Recuperado el 9 de diciembre del 2013, de http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Vulnerabilidad-Seguridad-informatica.php
- *Todo lo que quisiste saber sobre el mundo hack. (2001*). Recupero el 13 de diciembre del 2013, de http://delitosinformaticos.com/hacking/introhack2.shtm
- *Hacker, Cracker, Lamer, Defacer, ScriptKiddie, Newbie, Phreaker.(2010).* Recuperado el 14 de diciembre del 2013, de http://vateos.net/2010/02/hacker-cracker-lamer-defacer-scriptkiddie-newbie-phreaker/
- *Conoce a tu enemigo. (200).* Recuperado el 15 de diciembre del 2013, de http://his.sourceforge.net/honeynet/papers/enemy/
- *Definición de hacker, lammer, cracker, copyhacker, bucaneros. (2008).*Recuperado el 15 de diciembre del 2013, de https://docs.google.com/document/d/1-LayqBQAHKrPJ15FbbiPh86rW3rl--MBpV-Lkb1YYnU/edit?pli=1
- *Elevación de privilegio. (s.f.).* Recuperado el 17 de diciembre del 2013, de http://msdn.microsoft.com/es-es/library/aa751843(v=vs.110).aspx
- *Lo que necesita saber sobre la seguridad de su red. (s.f.).*Recuperado el 18 de diciembre del 2013, de

http://www.cisco.com/web/ES/solutions/smb/products/security/security_primer.html

- *Parrella, J. (2011).*Recupero el 19 de diciembre del 2013, de http://bitscloud.com/2011/05/como-defenderse-ataque-informatico/
- *Villa, G. (2013).* Recuperado el 20 de diciembre del 2013, de http://www.slideshare.net/Tensor/ataque-man-inthemiddle-25926293
- *Marco teórico. (s.f.).* Recuperado el 19 de diciembre del 2013, de http://virtual.urbe.edu/tesispub/0092449/cap02.pdf
- Universidad de Alcalá. (s.f.). *Niveles de seguridad.* Recuperado el 3 enero del 2014, de https://portal.uah.es/portal/page/portal/proteccion_datos/niveles_seguridad.