

## Botnet, la amenaza invisible

**Autor:** Ing. Roiman Valbuena

Universidad Rafael Bellosó Chacín, Maracaibo. Venezuela.

[www.urbe.edu](http://www.urbe.edu)

Universidad del Zulia, Maracaibo. Venezuela

[www.luz.edu.ve](http://www.luz.edu.ve)

[roybscomputers@yahoo.com](mailto:roybscomputers@yahoo.com)

[roybscomputers@hotmail.com](mailto:roybscomputers@hotmail.com)

**Fecha Publicación:** 13 de septiembre de 2008

**Este documento fue desarrollado especialmente para** [www.segu-info.com.ar](http://www.segu-info.com.ar)

## Indice

Botnet, la amenaza invisible .....	1
Indice .....	2
Introducción .....	3
La amenaza invisible de la tecnología Botnet.....	3
Defendiéndonos de las Botnets.....	4
¿Cómo trabaja el Asesino Web App? .....	5
Evolución de las redes botnets: Diferentes Arquitecturas .....	6
La botnet Pretty Park: .....	7
SubSeven Trojan/Bot .....	7
GT Bot.....	7
SDBot .....	8
La mayor amenaza proviene de las fallas en las legislaciones internacionales .....	8
Leyes Penales en Estados Unidos: .....	9
Brasil .....	10
India .....	10
República Popular de China .....	10
Conclusión .....	10
REFERENCIAS .....	11

## Introducción

El tema al cual se hace referencia en el presente artículo versa sobre muchos de los aspectos a considerar en el desarrollo de la tecnología botnet, cómo trabajan, breve descripción de su evolución, casos y sentencias penales reales. Al final se hace una evaluación de las leyes internacionales con respecto a la seguridad de los datos y se exponen algunos criterios del porqué esta tecnología se ha desarrollado tanto, prácticamente sólo conseguimos defendernos de ella, pero no hay vestigios de que podamos derrotarla.

## La amenaza invisible de la tecnología Botnet.

A lo largo del 2006, en diversas conferencias sobre técnicas de seguridad se discutieron las últimas "killer Web app", o aplicaciones Web. Y nos preguntaremos ¿pero que son estas cosas?, bueno, en definitiva, en la ingeniería software se denomina aplicación Web a aquellas aplicaciones que los usuarios pueden utilizar accediendo a un servidor Web a través de Internet o de una intranet mediante un navegador.

En el mismo orden de ideas, es una aplicación software que se codifica en un lenguaje soportado por los navegadores Web (HTML, JavaScript, Java, etc.) en la que se confía la ejecución al navegador. En el caso de las killer Web App, utilizan este navegador para detener ciertas aplicaciones que le sean adversas al creador del malware, y en su mayoría se basan en programas o software (pero podrían ser algo más) que son tremendamente exitosos.

Dicho de otra manera, es cualquier programa que ejecuta una solicitud en un computador, en la generalidad de los casos solicitudes manejadas remotamente, y que están diseñados para detener aplicaciones específicas, siendo su principal objetivo el software antivirus o los firewall [1]. Pero entonces nos preguntamos, ¿existen tales cosas?

Sí, existen, pero son pocas y dispersas. Todos los días, cientos si no miles de programadores, innovadores, empresarios, inventores y charlatanes trabajar duro para crear la próxima killer app.

Lamentablemente, esta tecnología Web, trabaja para los chicos malos, con financiamiento de la delincuencia organizada y los señores del spam [2], una generación de talentosos hackers sin moral que han creado un devastador arsenal de mortales juguetes, en forma de botnets.

Norman Elton y Matt Keel del William & Mary College [3], en 2005 en la presentación de su ponencia; **Who Owns Your Network?**, ¿Quién es el propietario de su red? Redes llamadas Botnets, expresaron que estas son: **"la mayor amenaza que enfrenta la humanidad."**

Esto puede ser una exageración, pero las redes botnets son sin duda la mayor amenaza con la que la comunidad de Internet se ha enfrentado.

John Canavan [4], en su artículo titulado "The Evolution of Malicious IRC Bots", enuncia que las botnets son **"La más peligrosa y extendida amenaza viral Win32"** Y concuerda mucho con la portada de la revista eWEEK de 16 de octubre de 2006, "Perdiendo la guerra botnet" [5].

El artículo de Ryan Naraine [6] titulado "¿Está la batalla botnet ya perdida?" [6], Describe el estado actual del medio ambiente de las botnet.

Las botnets son la clave central de los anillos de la delincuencia organizada en todo el mundo, pasan del robo de ancho de banda de redes zombies a ganar dinero infame de la actividad delincriminal en la Internet.

Un vendedor (en ebay.com de tecnología botnet y ataques de DDoS) dijo [7], que la calidad de su producto depende de la calidad de sus fuentes de inteligencia y, a continuación, pasó a decir que no podían suministrar ninguna información que pudiese responder por la calidad de sus fuentes de inteligencia. Siendo estas fuentes de inteligencia, los propios encargados de la seguridad dentro de las empresas que compran sus productos. Pero las botnets también pueden causar daños no intencionados [8].

A ver si nos entendemos, las redes botnet son el mayor peligro con los que se ha enfrentado la comunidad de Internet, como se dijo en párrafos anteriores, pero hay empresas que están desarrollando tecnologías para organizaciones delictivas [9], por el simple hecho de que es más productivo venderle a un delincuente, que venderle a un usuario particular, pero mejor que todo ello es, venderles a ambos.

Estas empresas tienen un negocio bien redondo, por un lado hacen creer a sus clientes que les están vendiendo lo último para protegerse, y al delincuente le transfieren las vulnerabilidades que previamente fueron dejadas intencionalmente abiertas por ellos mismos, a la final si no se comprueba que hubo delito en la venta, el cliente incauto volverá a comprar más Tecnología a la misma empresa que previamente los estafó, y el ciclo nefasto se repetirá.

## Defendiéndonos de las Botnets

Nuestras primeras armas contra las botnets deben consistir en eliminar el servidor bot, esta estrategia se conoce como "Eliminar la cabeza de la serpiente." Artículos recientes sobre el estado de la seguridad de las redes han lamentado el descubrimiento de que no estamos luchando contra una serpiente, sino por el contrario, un dragón de muchas cabezas, tal como en el Apocalipsis [10].

Se ha hablado mucho de la pérdida de esta arma por la prensa. En varios artículos se ha expresado que profesionales de la seguridad están admitiendo que esta batalla se está perdiendo [5]. En la guerra real, los generales deben dar batalla al enemigo, y no menos importante, deben luchar contra la pérdida de la moral. Muchos de los profesionales de la seguridad, que fueron pioneros en la lucha contra botnets, se han desmoralizado por la toma de conciencia de que el Mando y Control (C & C) del servidor ya no es tan eficaz como lo era antes.

Imagine como el primer ejército invasor que ha tropezado con un castillo debió sentirse. Imagine la reacción del propietario del castillo cuando se inventó la torre de asedio, o catapulta. Después de los años siguientes a la presentación de estas armas, el castillo pudo haber cambiado de diseño. Una sola pared que rodeaba el castillo se convirtió en una serie de torres. El castillo de forma rectangular, dio paso a formas irregulares destinadas a desviar en lugar de detener las armas del enemigo. La pérdida de una de las principales armas no significa la

pérdida de la guerra a menos que el general permita que la moral se disuelva, y no evoluciona para satisfacer el nuevo entorno.

## ¿Cómo trabaja el Asesino Web App?

¿Cómo hacer de una botnet un "killer app Web?" El software que crea y gestiona una botnet hace que esta amenaza sea mucho mayor que la anterior generación de código malicioso. No se trata simplemente de un virus, sino que es un virus de virus, o para simplificar un "Megavirus".

Una botnet es modular y un módulo explota las vulnerabilidades que encuentran para hacerse con el control sobre su destino. A continuación, se descarga otro módulo que protege al anterior, este es un nuevo robot que se encarga de detener el software antivirus y firewalls, el tercer módulo puede comenzar el escaneo de otros sistemas vulnerables [11].

Una botnet es adaptable, puede ser diseñado para descargar diferentes módulos, que a su vez explotan cosas específicas que encuentra en una víctima.

Por otro lado, nuevos exploits se pueden añadir tal cual son descubiertos. Ellos hacen el trabajo del antivirus mucho más complejo.

Encontrar un componente de una botnet no implica el carácter de cualquiera de los otros componentes debido a que el primer componente puede elegir para su descarga desde cualquier número de módulos para llevar a cabo la funcionalidad de cada una de las fases del ciclo de vida de una botnet.

Así mismo también arroja dudas sobre la capacidad de un software antivirus al afirmar que un sistema está limpio, cuando encuentra limpio uno de los múltiples componentes de un bot. Pero no es capaz de limpiarlos todos.

Debido a que cada componente se descarga cuando es necesario después de la infección inicial, las posibilidades de un sistema para obtener un exploit cero días es mayor.

Hay que hacer notar que si usted se encuentra administrando la seguridad del servidor de una empresa, está tomando el riesgo de poner un bot de nuevo en circulación si los esfuerzos para limpiar el código malicioso no son exhaustivos. En lugar de tomar ese riesgo, muchos departamentos de TI optan por volver a la imagen de un sistema conocido como imagen limpia, y créanme, esa no es la solución.

En efecto, los ataques botnet son directos. Es decir, el hacker puede orientar su ataque a una empresa o un sector de la misma. Aunque las botnets pueden ser aleatorias, también pueden ser personalizadas para un determinado conjunto de posibles anfitriones.

El **botherder** (el bot principal) puede configurar los bot clientes para limitar el direccionamiento IP de un conjunto predefinido de sus anfitriones. Con esta capacidad de orientación viene la capacidad de personalizar los ataques al mercado.

La capacidad de adaptación de los ataques de botnets es realmente buena. El bot cliente puede comprobar la acogida de los nuevos infectados, y de allí comenzará a hacer las solicitudes para explotar el sistema.

Cuando se determina que el anfitrión es propietario de un cliente, por ejemplo, una cuenta e-gold, el cliente puede descargar un componente que llevará en sus hombros durante las próximas conexiones a esa cuenta e-gold que el mismo realizará.

Lo más importante, si bien el titular de acogida está conectado a su cuenta e-gold, en el trasfondo se explotan los fondos de la cuenta mediante la presentación de una transferencia electrónica.

En un informe de amenazas de Internet (Septiembre 2006) [12], publicado por Symantec, el mismo afirma que durante los seis meses del período comprendido entre enero y junio de 2006, Symantec observó 57,717 redes bot activas por día. Symantec también observó que más de 4,5 millones de distintas redes de ordenadores podrían ser posibles redes bots de computadores, próximas a activarse.

Todo esto contrasta con un artículo publicado por este mismo autor en <http://seguridaddigitalvenezuela.blogspot.com/2008/08/ms-fraudes-online-en-el-primer-semestres.html>, y obtenido de <http://blog.s21sec.com>, que hace referencia al aumento de los fraudes online durante el primer semestre del 2008. Si bien se están haciendo grandes esfuerzos en controlar la expansión de las botnets, la realidad es que estamos muy lejos de eso.

Y podríamos perder la guerra si no tomamos conciencia de ello y nos preparamos para contraatacar.

## **Evolución de las redes botnets: Diferentes Arquitecturas**

La historia de las redes-zombi empezó en los años 1998-1999, cuando aparecieron los primeros programas que actuaban como Backdoor, así tenemos al conocido NetBus y BackOrifice 2000, a los puede llamar “pruebas de concepto”, es decir, programas en los que se usaban soluciones tecnológicas nuevas.

NetBus y BackOrifice 2000 fueron los primeros en tener una serie de funciones para el control a distancia del ordenador infectado, lo que permitía a los malhechores trabajar con los archivos en un ordenador a distancia y poner en funcionamiento nuevos programas, realizar capturas de pantalla, abrir y cerrar el dispositivo CD, etc.

Después, a alguno de los malhechores se le ocurrió hacer que las máquinas infectadas por los backdoors se conectaran por sí mismas y entonces se las podía ver siempre en línea (la única condición era que estuvieran encendidas y funcionando). Lo más seguro es que haya sido idea de algún hacker, ya que los programas zombi (bots) de la última generación usaban el canal de conexión que tradicionalmente usan los hackers - IRC (Internet Relay Chat).

### ***La botnet Pretty Park***

En mayo de 1999, fue descubierto Pretty Park, un bot cliente escrito en Delphi, de acuerdo con "The Evolution of Malicious IRC Bots", escrito por John Canavan de Symantec [4]. Este bot ya manejaba varias funciones y conceptos muy comunes en los robots de hoy, algunos son:

- La capacidad para recuperar el nombre del ordenador, versión del sistema operativo, información de los usuarios, y el sistema básico de información.
- La capacidad para buscar y recuperar las direcciones de correo electrónico y nombres de acceso ICQ
- La capacidad para recuperar los nombres de usuario, contraseñas, y dial-up de configuración de red
- La capacidad de auto-actualizarse
- La capacidad de carga / descarga de archivos
- La capacidad para poner en marcha una serie de ataques de DoS

### ***SubSeven Trojan/Bot***

En Junio, 1999, la versión 2.1 del troyano SubSeven fue liberada [13]. Esta versión fue significativa, ya que permitía que un servidor SubSeven pudiese ser controlado a distancia por un bot conectado a un IRC servidor.

Esto creó las condiciones para todos los botnets maliciosos que estaban por venir. SubSeven es un control remoto Trojan, también escrito en Delphi, promocionado por su autor como una herramienta de administración remota.

Su conjunto de herramientas, sin embargo, incluye herramientas que un verdadero administrador podría no usar, como la capacidad para robar contraseñas, registro de las pulsaciones de teclado, y ocultar su identidad. SubSeven dio control total a los bots operadores sobre los sistemas infectados.

### ***GT Bot***

Global Threat (GT), es una botnet cliente basada en mIRC [14], apareció en 2000. Fue escrito por Sony, MSG, y DeadKode. mIRC es un paquete software de IRC. mIRC tiene dos características importantes para la construcción de una botnet: Puede ejecutar scripts en respuesta a los acontecimientos en el servidor IRC, y soporta conexiones TCP y UDP.

Gt Bot posee las siguientes características:

- Escaneo de puertos en busca de formas de acceso
- Flooding: para conducir ataques de DDoS
- Cloning: la clonación es cualquier conexión a un servidor IRC, por encima de la primera conexión.
- BNC (Bounce): es un método de anonimato Bot para el acceso de los clientes a un servidor.

Hoy en día, todas las variantes de la tecnología bot que se basan en mIRC, se dice que son miembros de la familia GT Bot. Estos bot clientes no incluyen un mecanismo de propagación propia directamente. En lugar de ello, se utilizan variaciones en tácticas de ingeniería social.

### **SDBot**

A principios del 2002, apareció sdbot. Fue escrito por un programador ruso conocido como sd. Sdbot representó un paso importante en la cadena evolutiva de estos robots. Fue escrito en C++, posterior a ello el autor libera el código fuente y lo publica en una página Web, además de eso provee su email y su ICQ para información de contacto. Esto lo hizo accesible a muchos hackers y se hizo mucho más fácil de modificar y mantener.

Como resultado de esto, subsecuentes bots clientes incluían códigos o conceptos de sdbot. SdBot generaba un pequeño archivo binario de sólo 40kb. La mayor característica de la familia sdbot, fue la inclusión del uso de control remoto para backdoors. Varios años después, algunas de sus variantes todavía siguen causando daños [15].

Los siguientes backdoors son explotados por sdbot:

- Optix backdoor (puerto 3140)
- Bagle backdoor (puerto 2745)
- Kuang backdoor (puerto 17300)
- Mydoom backdoor (puerto 3127)
- NetDevil backdoor (puerto 903)
- SubSeven backdoor (puerto 27347)

En caso de que un exploit logre ser exitoso, el gusano crea y ejecuta un script que descarga sdbot en la nueva víctima y lo ejecuta. Una vez ejecutado, la nueva víctima es infectada. Ahora bien, Tengamos en cuenta que muchos de estos ataques se siguen utilizando hoy día, sobre todo el de la fuerza bruta, y el tratar de adivinar las contraseñas con ataques dirigidos a los puertos 139, 445, y 1433.

## **La mayor amenaza proviene de las fallas en las legislaciones internacionales**

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha establecido la necesidad de regulación por parte del derecho.

En nuestro caso Venezuela, existe la “Ley Especial Contra los Delitos Informáticos” [16], de fecha 30 de Octubre de 2001, la cual sólo contiene 33 artículos (deja por cierto una brecha muy grande para la impunidad de los hackers) estableciendo una prisión máxima de 2 a 6 años cuando se cometan delitos



tipificados en ella. Pero en esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir cómo se realizó dicho delito.

La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.

La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información.

En este punto debe hacerse énfasis y anotar lo siguiente:

- No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.
- No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.
- La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.
- Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y, todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.

### ***Leyes Penales en Estados Unidos:***

El derecho penal en Estados Unidos de Norteamérica conforma el fundamento para las investigaciones de delitos por computadoras llevadas a cabo por las autoridades federales (principalmente el FBI y el Servicio Secreto). Mientras que el 18 US Code 1030 es el decreto o ley principal contra los delitos computacionales [17].

**Abuso y Fraude por Computadora:** la sección a-) de la ley define el delito como el acceso intencional a una computadora sin la autorización para hacerlo. Por cierto que esta misma ley deja entrever que no se prohíbe específicamente obtener acceso a una computadora si el daño que se le hace no excede los 5.000 dólares. Sí así como está pensando, un intruso puede obtener acceso a las computadoras que quiera siempre que los daños que cause no sobrepasen esta suma (Eric Maiwald, 2003).

**Fraude con Tarjetas de Crédito:** El (18 US Code 1029), esta ley considera un delito apoderarse de 15 o más tarjetas de crédito falsificadas. Un ataque a un sistema de cómputo que permite que el intruso obtenga acceso a una gran cantidad de números de tarjetas de crédito para lo cual no tiene acceso autorizado es una violación a esta ley. Podría entenderse que cualquiera que se apodere de 10 tarjetas de crédito falsificadas no estaría cometiendo delito alguno, según esta ley.

**Intercepción (18 Code 2511):** El 18 US Code 2511 es una ley contra la intervención de las comunicaciones: Esta ley prohíbe la intercepción de llamadas telefónicas y otros tipos de comunicación electrónica, y evita que los agentes de la ley hagan uso de la intervención sin una orden judicial. No obstante, un intruso en un sistema de cómputo que coloca un “rastreador” en el sistema, probablemente este violando esta ley.

La lectura de esta ley también puede indicar que ciertos tipos de seguimientos realizados por las organizaciones puedan ser ilegales. Por ejemplo, si una organización coloca equipo de seguimiento o monitoreo en su red para examinar el correo electrónico o para vigilar los intentos de intrusión, ¿Constituye esto una violación a esta Ley?

### ***Brasil***

Tiene identificados dos delitos: la introducción de datos falsos en el sistema de información y la modificación o alteración no autorizadas de un sistema de información. Ambos están dirigidos a los empleados de organizaciones que hacen mal uso de su acceso para cometer un delito [17].

### ***India***

La manipulación de sistemas computacionales ajenos (“hacking”) con un sistema de cómputo está tipificado como un delito en la India.

Para ser culpable de este delito un individuo debe estar involucrado en la destrucción, eliminación o alteración de información en un sistema de cómputo de manera que reduzca su valor. El individuo también debe haber hecho el intento de causar daño, o debe saber que probablemente se iba a provocar un daño.

### ***República Popular de China***

El decreto número 147 del Consejo Estatal de la República Popular de China, del 18 de febrero de 1994, define dos delitos computacionales. El primero es la introducción deliberada de un virus de computadora en un sistema de cómputo. El segundo es la venta de productos especiales de protección de seguridad de computadoras sin permiso [17].

### **Conclusión**

De la evaluación de estas leyes, y por todo lo anteriormente planteado surge la incógnita, ¿Cómo combatir el delito informático en este mundo globalizado, cuando lo que es delito en un país no lo es en otro?, ¿cómo unificar criterios y hacer frente a las nuevas formas de fraudes informáticos cuando son las mismas empresas que generan y diseñan estas tecnologías las más sospechosas?

Indudablemente estamos ante amenazas de proporciones bíblicas, si se logra cerrar un agujero digital inmediatamente se abre uno más, y más complejo que su predecesor.

Este artículo se redactó con el fin de hacer referencia a la amenaza invisible que representa la tecnología botnet, y créanme, no hay nada más peligroso que luchar contra algo que no se ve.

## Referencias

- [1] Virus para detener Antivirus y Firewalls  
<http://www.enciclopediavirus.com/virus/vervirus.php?id=3762>
- [2] Arrestados tres controladores de botnets  
<http://www.enciclopediavirus.com/noticias/verNoticia.php?id=822>
- [3] Ponencia: Who Owns Your Network?  
[http://www.osc.edu/oarnet/oartech/meeting\\_min/it\\_william\\_mary.ppt](http://www.osc.edu/oarnet/oartech/meeting_min/it_william_mary.ppt)
- [4] Autor de varios libros de Seguridad en redes  
Fundamentals of Network Security John E. Canavan, 319 pages, Boston, London: Artech House 2001, ISBN 1-58053-176-8
- [4] John E. Canavan  
[http://www.symantec.com/avcenter/reference/the\\_evolution\\_of\\_malicious IRC\\_bots.pdf](http://www.symantec.com/avcenter/reference/the_evolution_of_malicious IRC_bots.pdf)
- [5] Artículo: Loosing the botnet war  
<http://www.securitypronews.com/news/securitynews/spn-45-20061024LosingTheBotnetWar.html>
- [6] Artículos escritos por: Ryan Naraine  
<http://www.eweek.com/cp/bio/Ryan-Naraine/>
- [6] Artículo: Está la batalla botnet ya perdida?  
<http://www.eweek.com/c/a/Security/Is-the-Botnet-Battle-Already-Lost/>
- [7] Anthony Scott Clark encontrado culpable de vender su tecnología  
<http://www.usdoj.gov/criminal/cybercrime/clarkPlea.htm>
- [7] Cae el supuesto cabecilla de catastrófica red zombi  
<http://www.viruslist.com/sp/news?id=208274109>
- [8] Caso Christopher Maxwell  
<http://www.usdoj.gov/criminal/cybercrime/maxwellPlea.htm>
- [9] Caso Napster  
<http://www.usdoj.gov/criminal/cybercrime/napsterbr.htm>
- [10] White Papers Killing Botnets McAfee  
<http://whitepapers.silicon.com/0,39024759,60285515p,00.htm>
- [11] Para más información sobre el funcionamiento léase el artículo de Lic. Cristian Borghello: "Botnets, redes organizadas para el crimen"  
<http://www.eset-la.com/threat-center/1573-botnets-redes-organizadas-crimen>
- [12] Informe de Amenazas de Internet Symantec 2006

[http://www.symantec.com/es/es/business/library/article.jsp?aid=latest\\_threat\\_findings](http://www.symantec.com/es/es/business/library/article.jsp?aid=latest_threat_findings)

[13] Versión nueva del troyano Subseven

<http://www.vsantivirus.com/sub722.htm>

[14] programa para IRC Internet Relay Chat

<http://www.mirces.com/>

[15] "sdbot.apa"

<http://www.laflecha.net/canales/seguridad/noticias/200503183>

[16] Ley Especial contra delitos informáticos en Venezuela

<http://www.tsj.gov.ve/legislacion/ledi.htm>

[17] Maiwald, Eric. Fundamentos de seguridad de redes. Segunda Edición. México, D.F. McGraw Hill. 2005. 473 p. ISBN: 9701046242.