ANALISIS COMPARATIVO DE LAS PRINCIPALES TECNICAS DE HACKING EMPRESARIAL

Comparative analysis of the main business hacking techniques

JHON F DUQUE B
Ingeniero de Sistemas.
Universidad Tecnológica de Pereira
jhonfduque@gmail.com

LARRY ANDRES SILVA
Ingeniero de Sistemas.
Universidad Tecnológica de Pereira
lasc1981@hotmail.com

EDYS DALIZA RENTERIA
Ingeniero de Sistemas.
Universidad Tecnológica de Pereira
edwys2@gmail.com

RESUMEN

En el presente artículo se presenta el problema del acceso al conocimiento de las fuentes de riesgo empresarial frente al concepto del hacking y sus posibilidades de solución, partiendo de los inconvenientes en materia de seguridad y la incidencia de estos en todo el entorno organizacional. Se abordan los conceptos de hacking y empresa y la relación existente entre ellos junto con las políticas de seguridad para la protección de la información. Así mismo se toman en cuenta los riesgos y análisis de estos riesgos como punto de partida para conocer las probabilidades de que las amenazas se concreten, y el impacto que generan.Seguidamente se muestran los pasos a seguir por la organización para implementar la seguridad informática de acuerdo a los riesgos que se presenten. Por último se dan a conocer las técnicas de Hacking más importantes, con sus objetivos de ataque, sus consecuencias y la manera más acertada de prevenirlas y/ó detectarlas.

PALABRAS CLAVES: amenaza, detección, empresa, Hacking, información, prevención, riesgo, seguridad, técnica, tecnología.

ABSTRACT

This article presents the problem of access to knowledge of the sources of business risk to the concept of hacking and its possible solutions, based on the disadvantages in safety and the incident of these around the organizational environment. The concepts of hacking and company, the relationship between them along with the security policies of the protection of information. Also takes into account the risks and analysis of these risks as a starting point to understand the threats likely to materialize, and the impact they generate. Following are the steps to be followed by the organization to implement information security according to the risk that arise. Finally, the article talks about the most important hacking techniques, with their targets of attack, its consequences and the most successful way to prevent and or detect them.

KEYWORDS: Company, detection, hacking, information, prevention, risk, security, technique, technology, threat.

1. INTRODUCCIÓN

Los protocolos de comunicación utilizados carecen (en su mayoría) de seguridad o ésta ha sido implementada en forma de "parche" tiempo después de su creación. Sea cual sea el ataque, por lo general cada una de estas intrusiones redunda en importantes pérdidas económicas para las organizaciones, además de la imagen negativa y poco confiable que esta daría ante sus inversionistas y administradores; esto debido a que cada empresa debe garantizar que todos sus recursos informáticos se encuentren debidamente disponibles al momento de requerir cualquier tipo de información y así poder cumplir con sus propósitosy para ello no puede haber alteraciónó manipulación por parte de factores externos.

Actualmente las empresas están expuestas a una gran cantidad de amenazas que vulneran sus sistemas informáticos, de allí la importancia de mantener la seguridad de los sistemas puesto que las consecuencias de un ataque informático pueden poner en riesgo la integridad de la información.El principal problema no es de carácter técnico sino de toma de consciencia de los peligros potenciales en la transmisión de información confidencial y el desconocimiento de las distintas técnicas de hacking empresarial.

Para las empresas lo más importante es la información.Se puede decir que la información es uno de los pilares más

Fecha de Recepción: (Letra Times New Roman de 8 puntos)
Fecha de Aceptación: Dejar en blanco

trascendentales a la hora de toma de decisiones en una entidad. De allí el valor que tiene para estos entes la protección y prevención de los sistemas de información.
Con el correr de los días se descubren más y más puntos débiles con opción de ser atacados y realmente son pocos los responsables de la información tecnológica que comprenden la importancia que tiene la seguridad informática para las organizaciones. Como si fuera poco carecen del conocimiento para abordar este grave problema que se forma a través de las vulnerabilidades que permiten a un atacante violar la seguridad de una organización y usar esta información para cometer delitos.
Existe una necesidad apremiante de proteger la integridad de la información de las organizaciones. Y es por ello que en el presente documento se realiza un análisis comparativo para conocer las principales técnicas de hacking empresarial mediante ayudas instructivas que permitan comunicar las posibles amenazas a los que se encuentran expuestos los sistemas de información de la organización.

2. HACKING EMPRESARIAL

La empresa se puede conceptualizar de diferentes maneras según Simón Andrade, autor del libro "Diccionario de Economía".La empresa es "aquella entidad formada con un capital social, y que aparte del propio trabajo de su promotor puede contratar a un cierto número de trabajadores. Su propósito lucrativo se traduce en actividades industriales y mercantiles, o la prestación de servicios".[1]Por su parte el Hacking se define como el conjunto de Técnicas y procedimientos utilizados por una persona con gran cantidad de conocimiento en el ámbito de la contra informática.
El avance de las tecnologías ha establecido otros patrones de delincuencia y por lo tanto es importante que, como ingenieros de sistemas, profesionales relacionados con esta área del conocimiento, empresas, trabajadores de la misma y/o usuarios, tomemos conciencia y seriedad frente a los problemas que pueden llegar a afectar no sólo nuestro empleo sino, peor aún, nuestra información en cualquier momento.
Existe una relación entre dos polos diametralmente opuestos: la criminalidad, como el mal más antiguo de la sociedad humana, y la tecnología informática y telemática, como los nuevos logros y conquista de la inteligencia humana. Como producto de esa relación, aparece un fenómeno que se ha denominado de la criminalidad informática[2],la cual emerge de las diferentes técnicas que normalmente son utilizadas por las personas para apoderarse de bienes ajenos.

La criminalidad informática no es más que una forma de quebrantar los sistemas de seguridad de una empresa, de modo que se pueda acceder a unos recursos u obtener una información deseada. Esto ha hecho que se incremente la necesidad de platear esquemas claros de protección sobre la información y demás recursos críticos de las empresas. Como si fuera poco, el hecho de prestar servicios que estén basados en interconexiones con diferentes redes, exige contar con políticas de seguridad robustas adicionales, que garanticen la prestación confiable de dichos servicios.
Tales políticas deben enmarcase dentro del contexto de una metodología de seguridad que trabaje sobre los principios básicos de seguridad: Autenticación,
Confidencialidad, integridad, disponibilidad, Control de acceso y Auditorias.
La seguridad informática es un área que día a día exige la presencia de un equipo capacitado y dedicado a esta labor, lo que conlleva a la especialización de las personas en diversos campos de la seguridad informática.

3. RIESGOS DE HACKING EMPRESARIAL

En el área de informática, existen riesgos a evaluar como son: ataque de virus, códigos maliciosos, gusanos, caballos de Troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.[3]
Cada díava en aumento la cantidad de casos e incidentes relacionados con la seguridad de los sistemas de información que comprometen los activos de las empresas. Las amenazas siempre han existido, la diferencia es que ahora, el enemigo es más rápido, más difícil de detectar y mucho más atrevido.
Por ello toda organización debe estar en alerta y saber implementar sistemas de seguridad basados en un análisis de riesgos para evitar o minimizar las consecuencias. Sin embargo es importante enfatizar que antes de implementar la seguridad, es fundamental conocer con detalle el entorno que respalda los procesos de negocio de las organizaciones en cuanto a su composición y su criticidad para priorizar las acciones de seguridad de los procesos claves de negocio más críticos y vinculados al logro de los objetivos de la empresa.

Un paso importante para implementar la seguridad de la información es el análisis de riesgos. Como su propio nombre lo indica, es realizado para detectar los riesgos a

[1] Promonegocios.net *http://www.promonegocios.net/mercadotecnia/empresa-definicion-concepto.html*
[2] Seguridad y delito informático

[3] http://www.ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm

los cuales están sometidos los activos de una organización, es decir, para saber cuál es la probabilidad de que las amenazas se concreten.
Las amenazas se pueden convertir en realidad a través de fallas de seguridad que deben ser eliminadas al máximo para que el ambiente que se quiere proteger esté libre de riesgos de incidentes de seguridad. Por lo tanto, la relación entre amenaza-incidente-impacto, es la condición principal a tomar en cuenta en el momento de priorizar acciones de seguridad para la correcta protección de los activosen la empresa.
Otro punto importante es la reciprocidad costo-beneficio. Este cálculo consiente en que sean evaluadas las medidas de seguridad con relación a su aplicabilidad y el beneficio que se logrará. Así, esta visión sitúa la implementación de las medidas de seguridad sólo en las condiciones en que la relación costo-beneficio se justifique.
Sin embargo, es fundamental que en la organización esté clara la relación costo-beneficio, es decir, que todos aquellos involucrados en la implementación de la seguridad (el equipo de ejecución del proyecto, la alta administración y todos sus usuarios) deben estar conscientes de los beneficios que las medidas de seguridad traerán para los individuos y para la organización como un todo.

4. TECNICAS DE HACKING

A continuación se presenta una clasificación de las diferentes formas de ataque, una evaluación de las posibles consecuencias que derivan de éstas, así como las maneras más acertadas de prevenirlas y contrarrestarlas.
En el primer grupo se ubican las técnicas de Monitorización que comprenden la etapa de observación.Estas son: Scanning(Escaneo de puertos), Enumeración del objetivo ySniffing (olfateo).
El Escaneo de puertos es el primer paso en la obtención deinformación básica sobre la red. Su objetivo es indagar por el estado de los puertos de un host conectado a una red, y si éstos puertos están abiertos analizar posibles vulnerabilidades.
Las consecuencias son constantes avisos del firewall y utilización maliciosa de puertos abiertos por parte de intrusos.
Es de suma importancia que todo esté bien configurado con aplicaciones que cubran todos los requerimientos y con unos buenos estándares de encriptación que aseguren la información, y un firewall que garantice el cuidado de los puertos.
Con la Enumeración del objetivo se recoge y organiza la mayor cantidad de información atinente a computadores, redes, aplicaciones y servicios. Al tener toda esta información organizada y disponible, lo que se pretende es avanzar a un siguiente estado donde el ataque cobra fuerza y los resultados van a ser inmediatos.
Los atacantes establecen conexiones activas con el sistema y llevan a cabo consultas dirigidas. Obtienen información en lo que respecta a máquinas, recursos de red, aplicaciones, y lo referente al sistema operativo.
Con el conocimiento de cualquier sistema el intruso puede preparar un ataque y acceder a todos los recursos informáticos. Este tipo de intromisión es el punto de partida para llevar a cabo ataques de Validación y de Modificación.
Para protegerse de ataques de enumeración se deben“configurar correctamente los servicios para que no muestren más información de la necesaria. No deben usarse nombres por defecto para archivos de configuración y hay que desactivar puertos de administración http y snmp”.[4]
Con el Sniffing se obtiene información de todo el tráfico que pasa por una red. En esta técnica “se usan analizadores de protocolos, que son programas que permiten monitorizar y analizar el tráfico de una red”[5]. Las aplicaciones descifran los paquetes de datos que viajan por la red y los almacenan para luego analizarlos. Entre toda esta información se pueden distinguir contraseñas, mensajes de correo electrónico, datos bancarios, y otros datos confidenciales de usuario.
Existen dos técnicas esenciales para lograr la detección de los sniffers. La primera se basa en el host, y es determinando si la tarjeta de red del sistema está funcionando en modo promiscuo. La segunda se basa en la Red. Igualmente, la información debe enviarseencriptada con algún tipo de tecnología como PGP ó GnuPG. Para evitar ataques en las redes se recomienda utilizar encriptación WPA. Si sólo se cuenta con WEP, la contraseña debe ser cambiada con regularidad. Los routers, también, deben estar bien protegidos con contraseñas.
En el segundo grupo se ubican las técnicas de Validación donde se “suplanta al dueño o usuario de la máquina mediante el uso de sus cuentan de acceso y contraseñas”.[6]
Una de ellas es el Ataque por fuerza bruta y se define como el procedimiento por medio del cual se intenta acceder a través de la obtención de la clave.Estos ataques se realizanobteniendo el archivo donde están todas las contraseñas encriptadas, y de manera offline se hallan todas las combinaciones posibles de dichas contraseñas.
Algunos sistemas no permiten acceder cuando se ha incurrido en cierto número de intentos fallidos. Sin embargo otros le hacen la vida fácil a quienes pretenden acceder con esta técnica, ya que utilizan las contraseñas más comunes.
Las medidas para defenderse contra los ataques por fuerza bruta permiten de cierta manera controlar el intento de acceso no autorizado.El más común de estos mecanismos es el denominado "regla de los

[4] Seguridad en VoIP: Ataques, Amenazas y Riesgos - Roberto Gutiérrez Gil - 2008
[5] Seguridad Informática: Técnicas hacker - Jesús Moreno León - 2010
[6] Sistema hibrido para la detección de código malicioso - Jorge Argente Ferrero - 2.009

1. Las notas de pie de página deberán estar en la página donde se citan. Letra Times New Roman de 8 puntos

tres strikes", que consiste enel bloqueo del acceso a una cuenta después de varios intentos de inicio de sesión fallidos (generalmente tres).[7]

En el Spoofing se suplanta la identidad de un dispositivo en una red informática para obtener información restringida.

Este ataque tiene algunas variedades entre las que se destaca el IP Spoofingque "consiste en generar paquetes de información con una dirección IP falsa".[8]Esta variedad de Spoofing tiene ciertas desventajas iniciales, como es el hecho de que el host víctima puede cortar la conexión o que los routersactuales no admiten paquetes cuyos remitentes no corresponden con los que administra en su red, lo cual acortaría el engaño a la red gestionada por un router.[9]

El riesgo más conocido de este ataque es el de Phishing, donde una persona es timada y se le hace creer que ha entrado a su entidad financiera de confianza.

Existen algunas medidas que se pueden utilizar para contrarrestar esta técnica que van desde el uso de IPsec para reducir los riesgos hasta la utilización de filtros que permitan asociar una dirección IP al tráfico que sale de la red en cuestión.

El Hijacking es una técnica por medio de la cual se intercepta y se roba una sesión de algún usuario para apropiarse de algún servicio.El atacante por medio de un software sniffer husmea los paquetes que están circulando por la red y envía paquetes al servidor, y con esto simula y se adelanta al usuario autorizado.

Como primera medida de protección se debe usar la encriptación, para que los datos que viajen por la red se encuentren codificados. No se puede dejar de lado el firewall, el antivirus y el antispyware.Los protocolos de seguridad tales como https son importantes también para evitar el robo de sesión.

La Ingeniería Social es un método basado en engaño y persuasión para obtener información significativa ó lograr que la víctima realice un determinado acto, como por ejemplo, ejecutar un archivo que le llegó por e-mail.[10]

Esta técnica es la que se usa con mayor frecuencia a la hora de indagar sobre nombres de usuarios y contraseñas. "Es un método que puede llevarse a cabo a través de canales tecnológicos (impersonal vía Internet o teléfono) o bien en persona, cara a cara"[11].

Algunas medidas a tener en cuenta son:

- Nunca divulgar información sensible con desconocidos ó en lugares públicos.
- Si se sospecha que alguien intenta realizar un engaño, hay que exigir que se identifique y tratar de revertir la situación intentando obtener la mayor cantidad de información del sospechoso.
- Llevar a cabo programas de concientización sobre la seguridad de la información.[12]

En los tipos de ataques D.o.S. se consigue que los servidores y redes informáticas colapsen y que de esta manera ya no puedan brindar sus servicios como lo hacen habitualmente.

La técnica Jamming se refiere al bloqueo de un canal de comunicación con la intención de impedir el flujo de información. "Aquí se satura al ordenador víctima con mensajes que requieren establecer conexión y dar respuesta. Como la dirección IP del mensaje puede ser falsa, la máquina atacada intenta dar respuesta a la solicitud de cada mensaje saturando su buffer con información de conexiones abiertas en espera de respuesta".[13]

Algunos elementos importantes para tener en cuenta a la hora de prevenir y descubrir ataques de Jamming son:

- La eliminación de las vulnerabilidades conocidas en los comportamientos del protocolo y la configuración del host.
- Filtrar el tráfico.
- La detección de ataques.[14]

El SynFloodingconsiste en mandar paquetes SYN a una máquina y no contestar a los paquetes ACK produciendo en la pila TCP/IP de la víctima una espera de tiempo para recibir la respuesta del atacante.[15]Mediante aplicaciones maliciosas se falsean las direcciones IP de origen, haciendo múltiples intentos de conexión desde un mismo equipo, lo que al hacerse en mayor escala llega a saturar el ancho de banda y colapsar los servicios que brindan el servidor. [16]

Entre las consecuencias están: Saturación de los recursos de memoria, incapacidad de establecer conexiones adicionales e inundación de puertos como Smtp y http.

Algunas medidas importantes son: Blindar el servidor con un firewall del tipo stateful, disponer de un sistema operativo actualizado y habilitar la protección SYN Cookie.

Las técnicas del tipo Modificación buscan la alteración no autorizada de los datos y ficheros de un sistema.

---

[7]Lightweight protection against brute force login attacks on web applications - http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=5593241

[8] Sistema hibrido para la detección de código malicioso - Jorge Argente Ferrero - 2.009

[9]Suplantación de la identidad - gpd.sip.ucm.es

[10]Hacking Etico - Carlos Tori - 2008

[11]Ibíd

[12]Ingeniería Social: Corrompiendo la mente humana - http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

[13] Sistema hibrido para la detección de código malicioso - Jorge Argente Ferrero - 2.009

[14]The dark side of the Internet: Attacks, costs and responses - http://www.sciencedirect.com.ezproxy.utp.edu.co/science/article/pii/S0306437910001328

[15] Sistema hibrido para la detección de código malicioso - Jorge Argente Ferrero - 2.009

[16] Sistema para Comunicación de Redes LAN, Inalámbricas y Bluetooth - AngelHaniel Cantú Jáuregui - 2008

El Borrado de huellas consiste en modificar los ficheros log del sistema operativo de la máquina asaltada, donde queda constancia de la intrusión, para borrar el rastro dejado por el atacante.[17]El intruso puede borrar sus rastros programando un zapper adecuado al objetivo y al modo de gestionar registros que existe en el servidor. A su vez, debe borrar todos los logs que éste modifica tras su paso y sólo eliminar las entradas que corresponden a dichas sesiones.[18]
Las consecuencias son: Posibilidad de ataque futuro, al no detectarse la intrusión a tiempo y pérdida de información de la mano del borrado de archivos.
En cuanto a medidas de protección,si se detecta al intruso pueden ocurrir tres cosas importantes. Lo primero es que sabiendo dónde está el hueco de seguridad, éste puede ser cubierto. Lo segundo es que con el conocimiento obtenido se pueden evitar ataques posteriores, y se puede llevar a cabo es el rastreo del atacante.

5. APORTES

El Hacking Empresarial se define como el conjunto de técnicas y procedimientos utilizados por una persona con gran cantidad de conocimiento en el ámbito de la contra informática.
La relación entre los riesgos y los ámbitos se especifica comparandoqué tan alto es el riesgo que se toma en cada una de las decisiones con respecto a los diferentes ámbitos.
Las técnicas de Hacking parten de cuatro grandes grupos que son: Monitorización, Validación, DOS (Denegación de Servicio) y Modificación. Cada una de las técnicas expone una definición, su objetivo, el modo de operación, sus consecuencias y cómo detectarla ó prevenirla.
El grupo de Monitorización está compuesto por Scanning (Escaneo de Puertos), Enumeración y Sniffing (Olfateo). Validación se compone de Fuerza bruta, Spoofing(Suplantación), Hijacking(Robo de sesión) e Ingeniería Social. En el DoS ubicamos las prácticas de Jamming (Interferencia) y SYN Flooding (Ataque por sincronización). Y finalmente en el grupo de Modificación encontramos el Borrado de huellas.
Se le brinda especial importancia al primer y segundo grupo de prácticas, ya que allí se gestan las bases para cualquier intrusión en un sistema informático. Del tercer grupo se analizan las dos técnicas más importantes y del último grupo se estudia la técnica con la cual finaliza cualquier ataque de Hacking.

6. CONCLUSIONES

Este trabajo ha descrito la naturaleza y características de la importancia de la seguridad informática en el tema de hacking empresarial, la importancia de implementar una cultura de seguridad informática empresarial y cuál es el impacto que esta traerá a la organización. Asimismo, se establecieron ciertos parámetros que ayuden a las personas a discernir acerca de la creación e implementación de una cultura de seguridad informática en ámbitos empresariales.
La información recogida acerca de las diferentes técnicas de Hacking permite abordar el problema del acceso sin autorización tanto desde una perspectiva de prevención como desde un ámbito de detección con las correspondientes medidas. Con el conocimiento adquirido se dispone de cierta ventaja para afrontar muchos de los retos que surgen cada día en materia de seguridad informática.
Se ha podido observar la gran cantidad de situaciones de amenaza en las que se encuentran inmersas las organizaciones, así como la necesidad de documentación y, más que eso, capacitación para todas las personas que forman parte de la organización, en busca de unos métodos y unas prácticas más eficientes. Este factor humano debe tomarse como el elemento clave, ya que de una adecuada sensibilización dependen los resultados a la hora de afrontar situaciones que ponen en riesgo la estructura organizacional.
Ahora queda en manos de los directivos de estas organizaciones el tomar las mejores decisiones que procuren en un largo plazo obtener altos logros en la defensa de sus sistemas de información con mecanismos de protección de la información y mecanismos de prevención.

7. RECOMENDACIONES

Es importante que de ahora en adelante se ahonde en el estudio de las prácticas de Hacking y que cada día se profundice en los alcances que tienen estas técnicas así como la manera de prevenir y contrarrestar sus efectos, descubriendo deficiencias en la seguridad y reaccionando para solucionar los inconvenientes que surjan.
No hay que olvidar la importancia de la prevención que parte de una concientización y buena capacitación a todas las personas encargadas desde los administradores hasta las secretarias. Esta participación mancomunada seguramente redundará en un buen funcionamiento del sistema que al bajar sus vulnerabilidades también bajará los costos que éstas implican.
En lo técnico es importante aunar y trabajar con dos elementos que a veces se tratan por separado. Por un lado están las herramientas de prevención que cuentan con la capacidad de bloquear las técnicas de los atacantes. Por otro lado, y no menos importante, se encuentran las herramientas de detección que centran su fortaleza en el análisis y pueden enfrentarse a los intrusos que intentan acceder de manera fraudulenta.

[17]Sistema híbrido para la detección de código malicioso - Jorge Argente Ferrero - 2.009
[18]Hacking Etico - Carlos Tori - 2008

1. Las notas de pie de página deberán estar en la página donde se citan. Letra Times New Roman de 8 puntos

8. REFERENCIAS BIBLIOGRAFICAS

- Promonegocios.net - http://www.promonegocios.net/mercadotecnia/empresa-definicion-concepto.html[Consulta: 12 de septiembre de 2011]
- Seguridad y delito informático
- Seguridad informática ¿Qué, por qué y para qué? - http://www.ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm [Consulta: 14 de septiembre de 2011]
- Gutiérrez R. Seguridad en VoIP: Ataques, Amenazas y Riesgos. Universidad de Valencia. 2008
- Moreno J. Seguridad Informática: Técnicas hacker. 2010 - http://informatica.gonzalonazareno.org
- Argente J, García R, Martínez J. Sistema híbrido para la detección de código malicioso. Departamento de Ingeniería del Software e Inteligencia Artificial - Facultad de Informática - Universidad Complutense de Madrid. 2009
- Adams C, Jourdan G, Levac J, Prevost F. Lightweight protection against brute force login attacks on Web applications. PST 2010; 181-188
- Núñez E, Villaroel C, Cuevas V. Suplantación de la identidad. Universidad Complutense de Madrid. 2010
- Tori C. El Hacking Etico. Argentina, 2008. 328 pag.
- Sandoval, E. Ingeniería Social: Corrompiendo la mente humana [artículo de Internet]. http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana [Consulta: 23 de septiembre de 2011]
- Kim W, Jeong O, Kim C, So J. The dark side of the Internet: Attacks, costs and responses.Inf. Sys. 2011; 36 (3): 675-705
- Cantú A. Seguridad Informática: Sistema para comunicación de Redes LAN, Inalámbricas y Bluetooth [Trabajo de Grado]. Tamaulipas: Universidad Autónoma.Facultad de Ingeniería; 2008. 123 p.