ANALISIS COMPARATIVO DE LAS PRINCIPALES TECNICAS DE HACKING EMPRESARIAL

LARRY ANDRES SILVA CASTRO
EDYS DALIZA RENTERIA CORDOBA
JHON FREDDY DUQUE BLANDON

UNIVERSIDAD TECNOLOGICA DE PEREIRA
PROGRAMA DE INGENIERIA DE SISTEMAS Y COMPUTACION
FACULTAD DE INGENIERIAS
PEREIRA
2011

ANALISIS COMPARATIVO DE LAS PRINCIPALES TECNICAS DE HACKING EMPRESARIAL

LARRY ANDRES SILVA CASTRO
EDYS DALIZA RENTERIA CORDOBA
JHON FREDDY DUQUE BLANDON

MONOGRAFIA PARA OPTAR AL TITULO DE INGENIERO DE SISTEMAS

PROFESOR ASESOR:

OMAR IVAN TREJOSBURITICA

UNIVERSIDAD TECNOLOGICA DE PEREIRA
INGENIERIA DE SISTEMAS Y COMPUTACION
FACULTAD DE INGENIERIAS
PEREIRA
2011

Notas de Aceptación

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Pereira, octubre del 2011

Contenido

LISTA DE TABLAS

LISTA DE FIGURAS

1 ANALISIS COMPARATIVO DE LAS PRINCIPALES TECNICAS DE HACKING EMPRESARIAL

1.1 DEFINICION DEL PROBLEMA

Los protocolos de comunicación utilizados carecen (en su mayoría) de seguridad o esta ha sido implementada en forma de "parche" tiempo después de su creación. A continuación se relacionaran algunos de los distintos tipos de ataques cometidos generalmente por Hackers. Son ataques que pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando los distintos protocolos:

- Ingeniería Social
- Ingeniería Social Inversa
- Ataques de autenticación
- Denial of Service (DoS)
- Ataques de modificación - Daño
- Códigos Maliciosos
- Spam
- Virus
- Troyanos
- Farming
- Fishing.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un sistema informático, y sea cual sea el ataque por lo general cada uno de estos 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 propósitos y para ello estos no pueden estar alterados o manipulados de mala manera por factores externos.[1]

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. Es muy importante tener en cuenta que las empresas u organizaciones no se pueden permitir el lujo de denunciar ataques a sus sistemas, pues el nivel de confianza de los clientes (ciudadanos) bajaría enormemente.[2]

Los ataques informáticos tienen gran incidencia negativa en varios sectores de la información de cada entidad, puesto que esta se podría ver modificada inadecuadamente, además de que se podría volver publica información privilegiada tanto de la organización como de sus clientes al dejar expuesta la información de sus usuarios, entre otros.

Un ataque informático puede ocasionar un gran caos en las empresas, simplemente basta con remitirnos al pasado 20 de abril del presente año cuando la empresa Sony se percató de que había recibido un nuevo ataque que expuso los datos de sus usuarios en línea, este fue el segundo caso de ataque que recibió la empresa Sony durante el presente año y del cual dejo expuesta la información personal de 24.6 millones de cuentas de sus clientes.

[1] http://www.buenastareas.com/ensayos/Amenazas-L%C3%B3gicas/2453279.html
[2] http://www.buenastareas.com/ensayos/Amenazas-L%C3%B3gicas/2453279.html

Debido a este acontecimiento la compañía japonesa se vio en la obligación de apagar sus plataformas mientras lograba garantizar que estás volvían a ser seguras, esto lógicamente ocasiono unas pérdidas económicas y de prestigio enormes.

De la misma manera se puede citar el ataque a la página de la presidencia de ecuador a nombre del grupo Anonymous, incluso este país donde se pensaba que los ataques cibernéticos eran asunto de otros países, una legión de ciberactivistas entró ilegalmente a las plataformas de una decena de instituciones públicas y privadas. Dicen no tener un líder oficial y como rostro muestran la máscara del anarquista revolucionario de V de Vendetta, la novela gráfica de Alan Moore. Pero sí tienen voces y se autodenominan Anonymous.

Es decir, son la extensión del colectivo internacional de hackers con igual nombre. Ano-nymous Ecuador ya cuenta con más de 100 integrantes que dicen ser menores de 30 años. No todos los miembros son hackers, solo una minoría son ingenieros en sistemas. La mayoría son ciberactivistas que participan de las conversaciones online, agrupados en varias cuentas de Facebook y Twitter.[3]

De igual manera Colombia sufrió con una serie de ataques informáticos, ya que este mismo grupo hackeo las páginas web de los ministerios de defensa y educación, así como el senado y las cuentas del presidente Juan Manuel Santos y el ex mandatario Álvaro Uribe.

El diario colombiano El Espectador señala que la serie de ataques empezó el pasado 16 de agosto y, según Anonymus, responde al hecho de que el ministro de Defensa de Colombia, Rodrigo Rivera, calificó de "terroristas informáticos" a

[3]http://wsp.presidencia.gov.co/Paginas/Presidencia.aspx

los hackers de la organización y en un mensaje difundido en Twitter, los ciberactivistas escribieron: "Presidencia, Senado, Min educación, Min defensa, Santos presidente, buen día señores!".

Mientras tanto el ciber ataque al ministerio de Educación es en protesta a un proyecto de reforma a la universidad pública, para que entren capitales privados. "El ministerio de Educación es el culpable de vender nuestra educación", dijeron los hackers a través de Twitter. "Porque mi educación no es una mercancía, yo le digo no a la nueva ley de educación superior", agregaron.

En Colombia según estadísticas durante el año 2007 las empresas perdieron más de 6.6 billones de pesos a raíz de los delitos informáticos, de allí que el 5 de enero de 2009, el congreso de la república de Colombia promulgo la ley 1273 "por medio de la cual de modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "De la Protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones ".[4]

En consecuencia las empresas se ven afectadas por problemas relacionados con la seguridad informática, ya que evidentemente la seguridad en Internet afecta de forma excesiva a las organizaciones que operan en la web como bancas electrónicas, por ejemplo las cuentas bancarias en internet no son más que bases de datos y, como tal, están expuestas. En definitiva, la seguridad afecta a todos: a las grandes compañías por ser una gran tentación para los hackers, los cuales ven en ellas una posible opción de filtración y a los usuarios individuales por su vulnerabilidad.

[4]http://www.tareanet.edu.co/index.php?option=com_myblog&show=ley-1273-de-2010-delitos-informaticos-3768.html&Itemid=

Por lo tanto con el presente trabajo de grado se pretende abordar el problema del acceso al conocimiento de las fuentes de riesgo empresarial frente al concepto del hacking y sus posibilidades de solución ya que gran cantidad de organizaciones están expuestas al ver como sus sistemas de información además de que son vulnerados por causas externas no cuentan con personal capacitado para minimizar este tipo de ataques.

Así pues 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.

1.2 JUSTIFICACION

Para las empresas lo más importante es la información, se puede decir que la información es uno de los pilares más 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 paso del tiempo la humanidad se ha encontrado con grandes avances a nivel tecnológico y de comunicaciones que han permitido que el mundo evolucione a pasos agigantados, y que cada día surjan más y mejores cuestionamientos acerca de lo que el ser humano es capaz de realizar con tal de satisfacer sus necesidades o por qué no sus gustos siempre buscando la comodidad y es por eso que se creó la Internet, la telefonía móvil con todo lo que implican sus avances en cuanto a equipos y servicios, avances en la medicina etc.

Así mismo es importante y notable manifestar como todos estos avances tecnológicos y de comunicación se han convertido en oportunidades hostiles de ataque, donde cada vez más personas intentan beneficiarse ilegalmente para obtener algún beneficio en su mayoría económico.

Actualmente podemos notar el cambio enorme que ha dado gran parte de la humanidad en torno al tema, pues hace algunos años atrás cuando apenas se concebían las ideas de desarrollo muchas de estas personas que contaban con grandes habilidades disfrutaban el hecho de aportar ideas en este campo informático, se disfrutaba realizando investigaciones que les permitieran adquirir mayor conocimiento y por ende avanzar en la culminación de cada una de las metas o ideas que se había planteado.

Hoy en día todo esto se ha desvirtuado completamente dando origen a nuevas personas que aprovechando su gran conocimiento en los medios informáticos y el manejo de sus herramientas las usan para delinquir de algún modo.

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 y peor aún 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.

La gran mayoría de estos ataques tienen como objetivo principal el sector empresarial sin importar la magnitud, el dinero y los sistemas de información que dichas organizaciones manejen, para los delincuentes informáticos todo es válido; se convierte en algo realmente necesario y de vital importancia construir e idear

estrategias de seguridad que permitan establecer algún tipo de barreras que admitan minimizar de manera efectiva ataques tanto externos como internos.

Se puede garantizar que los recursos informáticos de una compañía estarán disponibles si se tiene un claro conocimiento de las potenciales técnicas de hacking a las que estas se enfrentan, para cumplir sus propósitos, es decir, que no estén dañados o alterados.

Uno de los métodos para lograr mitigar eficazmente los impactos provocados por un ataque informático, es precisamente tener conocimiento de la manera como estos atacan y conocer los posibles puntos débiles de un sistema comúnmente explotados y en los cuales se debe hacer especial énfasis al momento de concentrar los esfuerzos de seguridad propensos a la prevención de los mismos.

Por lo tanto el presente trabajo de grado se justifica ya que existe una necesidad latente de proteger la integridad de la información de las organizaciones, este establecerá un análisis comparativo para prevenir las principales técnicas de hacking, conociendo las diferentes debilidades mayormente explotadas por quienes pretenden atacar y sobrepasar las barreras de la seguridad de los sistemas informáticos empresariales.

Utilizando esta documentación o ayudas instructivas que permitan comunicar las posibles amenazas en los sistemas de información a los que se encuentran expuestas las organizaciones, junto a posibles contramedidas por medio de las cuales es factible mitigar de manera efectiva los diferentes tipos de ataques que día a día recibe un sistema, garantizando la operatividad y competitividad de las empresas en el mercado.

En dicho análisis se ilustrara de una manera adecuada y detallada paso a paso la forma como cada individuo de la organización deberá asumir sus

responsabilidades en el manejo y manipulación de la información, así cada uno de estos sabrá proteger algo tan valioso para la empresa como lo son estos.

Por tanto, el presente trabajo de grado se justifica debido a la gran importancia que tiene el tema en el mundo empresarial moderno y a la necesidad de articular dichas realidades del mundo moderno con el perfil profesional del egresado de Ingeniería de Sistemas y Computación de la Universidad Tecnológica de Pereira.

1.3 OBJETIVOS

1.3.1 GENERAL

Construir un documento de 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.

1.3.2 ESPECIFICOS

- identificar los posibles ataques presentados en los sistemas de información empresarial.

- Comprender las debilidades más comunes que pueden ser aprovechadas y cuáles son los riesgos asociados, con el fin de ejecutar de manera inteligente y eficaz estrategias de seguridad efectivas.

- ❖ Conocer las diferentes etapas que conforman un ataque informático.

- ❖ Documentar una serie de pasos que permitan minimizar en un alto porcentaje los riesgos de un ataque informático a los que se ven expuestas las organizaciones.

1.4 MARCO DE REFERENCIA

Las metodologías de Hacking son temas que cada día tienen más acogida por parte de los profesionales de todas las ramas del conocimiento. En las empresas debido al aumento de amenazas, ha crecido el afán por conocer las formas de contrarrestar dichos peligros para que esto no se constituya en óbice en el desarrollo de cualquier organización.

Aun así muchas de estas empresas por desconocimiento de los diferentes tipos de amenaza no han logrado crear metodologías que les permitan salvaguardar sus datos e información y preparase para lo inevitable.

A continuación se desglosa el conjunto de términos que nos ubican en el contexto de las Técnicas de Hacking. Como Técnica se entiende el conjunto de procedimientos y recursos de que se sirve una ciencia o un arte, y la pericia o habilidad para hacer uso de esos procedimientos y recursos. Esta definición se encuentra en el Diccionario de La Lengua Española.[5]

[5]Diccionario de la Lengua española. http://buscon.rae.es/draeI/

El término Hacking en nuestros tiempos, para la mayoría de la gente y de la prensa, está ligada a delincuentes comunes, a personas de dudosa moralidad que utilizan conocimientos de informática o electrónica para delinquir.[6]

En un sentido más amplio podemos definirlo como un cúmulo de conocimientos relacionados con la seguridad y la vulnerabilidad de los sistemas informáticos, y la manera de aprovechar las falencias junto con las herramientas para protegerse de los ataques.

"Algunos de los daños causados y asociados al hacking son:

- Robo electrónico de fondos
- Invasión de la privacidad causada por la divulgación de información privada
- Angustia o daño psicológico causado por el acoso cibernético
- Pérdida de ingresos debido a la violación de los derechos de propiedad
- Pérdida de tiempo para instalar y gestionar la tecnología de defensa
- Daño físico por ser víctimas de pedófilos y la prostitución infantil
- Pérdida de dinero para pagar por la tecnología de defensa".[7]

En cuanto al daño físico y las situaciones que ponen en peligro la integridad de las personas existen sitios web que convocan a las personas para llevar a cabo suicidios masivos. En Corea del Sur, durante los últimos años, ha habido varios informes de dos o tres personas que se reunieron en los sitios Web de suicidio que se realizan masivamente.[8]

Desde un punto de vista de la personalidad, un hacker puede ser:

- Un empleado descontento
- Alguien con odio contra su compañía o compañeros de trabajo

[6]Hacking Etico - Carlos Tori - 2008
[7]The dark side of the Internet: Attacks, costs and responses - http://www.sciencedirect.com.ezproxy.utp.edu.co/science/article/pii/S0306437910001328
[8]Ibíd.

- Una persona con tedio

Sin embargo las razones financieras son las que más mueven a los individuos a llevar a cabo estas actividades de hacking.

En el documento Thedarkside of the Internet: Attacks, costs and responses, se recogen algunos elementos que mueven a los hackers, desde un punto de vista sicológico. El primero de ellos cita las emociones negativas que llevan a la gente a cometer delitos. La baja autoestima es otro de los elementos. La rivalidad con otros también se constituye en un elemento clave. Y por último, el estrés y la manera de liberarse de él.[9]

Existen algunos hechos históricos con respecto al Hacking, los cuales se citan a continuación.

> En el año 1982 John Shoch (uno de los creadores de Ethernet), junto a un colega, escribieron el primer reporte sobre un gusano (worm), tomando ese nombre de una novela de ciencia ficción de 1975 en la que, bajo el nombre Tape worms, describían a programas autómatas que viajaban por las redes transportando información. Para 1983 se estrenó la famosa película WarGames, en la que el actor Matthew Broderick interpretaba a un chico que ingresaba en una base militar a través de su computadora y casi desata una guerra nuclear.
>
> Un año más tarde se crearon la publicación 2600, el CCC chaos computer club, Legion of Doom y la División de fraude con tarjetas y computadoras del Servicio Secreto. Ya en 1988 Robert Tappan Morris soltó un gusano en Arpanet (como se llamaba Internet antes)

[9] Ibíd.

> y de ese modo infectó miles de servidores Unix. Fue enjuiciado y condenado a cumplir 400 horas de trabajo social.
>
> Años más tarde En 1992 Kevin Mitnick, luego de estar prófugo y ser atrapado por el FBI, fue sentenciado por robo de software e intrusiones en organizaciones. Y en 1994 Vladimir Levin robó, desde San Petersburgo, a través de los sistemas de Citibank, más de 10 millones de dólares por medio de transferencias a sus cuentas. En los dos años siguientes, desde otros bancos de los Estados Unidos, 300 millones de dólares se movilizaban electrónicamente de modo fraudulento[10]

Un Sistema informático se define como el conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son: hardware, software y las personas que lo usan.

Las tecnologías de seguridad cumplen el papel de apoyar la confidencialidad de todos los datos privados, con herramientas tales como cortafuegos, antivirus y así sucesivamente. En otras palabras, se trata de tecnologías de defensa, y sobre todo de las medidas de control de acceso.

Las herramientas de hacking se definen como aquellas tecnologías que se utilizan para probar las tecnologías de seguridad. Entre las herramientas de Hacking tenemos el escaneo de vulnerabilidad, los exploits, y los marcos de evaluación de la seguridad. Estos mecanismos de seguridad ofensiva se requieren con el fin de poder evaluar el nivel de seguridad de una infraestructura informática.[11]

[10] Hacking Etico - Carlos Tori - 2008

[11] The security and privacy impact of criminalising the distribution of hacking tolos - http://www.sciencedirect.com.ezproxy.utp.edu.co/science/article/pii/S136137230870112X

La diferencia entre las tecnologías de seguridad y las herramientas de Hacking radica en el uso que se les da. Las primeras se utilizan de una manera benigna, mientras que las otras se pueden utilizar de dos maneras, bien sea con fines beneficiosos, como en el caso del Hacking ético, o como una manera de ocasionar daños.

1.5 DISEÑO METODOLOGICO

A. HIPOTESIS

Es posible potencializar los mecanismos de seguridad de los sistemas informáticos empresariales en la medida en que se conozcan los riesgos a que está sujeta la información de una empresa.

B. VARIABLES

Parámetros de seguridad empresarial.

C. INSTRUMENTOS

No aplica

2 HACKING EMPRESARIAL

Antes de definir lo que es hacking empresarial debemos retomar dos conceptos claves que son la base para el desarrollo de nuestro capítulo. El cual va dirigido a divulgar debilidades y vulnerabilidades de los sistemas de información.

2.1 QUE ES UNA EMPRESA

La empresa se puede conceptualizar de diferentes maneras según el autor: 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"[12]

Otra definición es tomada del diccionario de Marketing, la cual define a la empresa como una "unidad económica de producción, transformación o prestación de servicios, cuya razón de ser es satisfacer una necesidad existente en la sociedad"[13]. Además admite integrar otros factores como recursos humanos, bienes materiales y aspiraciones.

En conclusión, la definición de empresa permite “concebir” a toda la empresa como una entidad conformada por 2 tipos de elementos entre los cuales están: elementos tangibles e intangibles.Los elementos tangibles se caracterizan por poseer (elementos humanos, bienes materiales, capacidad financiera y de

[12] Promonegocios.net *http://www.promonegocios.net/mercadotecnia/empresa-definicion-concepto.html*
[13] Ibíd.

producción, transformación y/o prestación de servicios), los intangibles describen (pretensiones, realizaciones y capacidad técnica); cuya finalidad es la satisfacción de las necesidades y deseos de su mercado; la cual a su vez es meta para la obtención de una utilidad o beneficio.

Figura 1. Delimitación de los oficios de la empresa

En la figura 1, se hace descripción de las áreas básicas que conforma una empresa, que como mencionamos anteriormente son los principios en los que se basa el hacking empresarial para definir lo que es una empresa. La capa superior de la pirámide, proporciona toda la parte de direccionamiento estratégico de la organización (objetivos a corto y largo plazo, metas, misión y visión) y como cada unas de las áreas tiene sus propios riesgos con la diferencia que estos pueden quebrar o no una empresa.

En las competencias y capacidades personales se busca medir las habilidades y destrezas que tienen los empleados en las organizaciones para realizar las tareas diarias y así poder cumplir los objetivos propuestos por la entidad. Las competencias y capacidades organizativas es el área encargada de velar que se realicen los procesos en forma adecuada y estructura la entidad de manera que

por medio de sus actividades este alcance un nivel y posicionamiento en el mercado por el cual compite.

Por último, la pirámide central es la base principal de desarrollo de los procesos y actividades que una organización proporciona a sus clientes, ya que esta sección de la empresa es un verdadero avance en diferentes áreas y en ellas se ve la necesidad de realizar gestiones de manera dinámica, eficiente y precisa.

Al aplicarse tecnología en todas las áreas se observan gestiones automatizadas, a la vez se establece un gran paso en la creación de mejores métodos y procedimientos que ayuden al personal de trabajo de las empresas a desempeñar más eficientemente las tareas que realiza en condiciones adecuadas y normales. Es aquí en la automatización, mejora y creación de nuevos procesos donde aparecen las grandes amenazas para estas organizaciones.

2.1.1 ¿QUÉ SE CONOCE COMO HACKING?

Es complicado dar un concepto unificado de lo que es hacking. Pero si se tiene en cuenta como las personas logran vulnerar la seguridad diseñada por los administradores de red e informática en las empresas. Se puede definir de la siguiente manera.

Conjunto de técnicas y procedimientos utilizados por una persona con gran cantidad de conocimiento en el ámbito de la contra informática; estas personas se caracterizan por tres aspectos: la diversión [1] por que se apasionan por lo que hacen de manera que cada día se enamoran más por lo que realiza. La otra es el talento [2] que son Habilidad innata o capacidad de comprender y entender estos sistemas informáticos para extraer los recursos o información de forma

adecuada. También se puede decir que es el potencial de un individuo para desempeñar muy bien actividades delictivas.

Por último tenemos la exploración[3] que es la búsqueda continua de aquellas debilidades o fallas (parches, errores) en los sistemas. En los cuales estas personas ven la oportunidad de demostrar sus habilidades para cumplir un determinado objetivo. De esta manera, hacking significa explorar los límites de lo que es posible en un espíritu de traviesa inteligencia. Esta palabra suele asociarse a procedimientos ilegales o malignos.

2.1.2 RELACION QUE HAY ENTRE HACKING Y EMPRESA

Para nadie es un secreto que la tecnología va avanzando, poco a poco, condicionando a muchas de las formas de vida características de los seres humanos. El avance de las tecnologías ha establecido otros patrones de delincuencias 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.[14] La cual emerge de las diferentes técnicas que

[14]Seguridad y delito informatico

normalmente son utilizadas por las personas para apoderarse de bienes ajenos a estos.

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 fuere 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. Esta metodología debe ser completa para que consienta desarrollar integralmente la seguridad en cualquier área de una empresa u organización.

En actualidad, muchas empresas caen en el error de que la seguridad se limita a proteger las redes y mantener antivirus actualizado en los equipos de la organización. La seguridad informática es un área que día a día exige la presencia de un equipo capacitado y dedicado a esta labor, lo que ha conllevado a la especialización de estas personas en diversos campos de la seguridad informática.

Ahora bien, todos reconocen la necesidad de tener alguna clases de control para que su información este propiamente respaldada. Sin embargo ellos mismos oponen resistencia a ser controlados y no sienten la urgencia de implementar las inspecciones hasta que los problemas se presentan de forma tangibles.

El desarrollo de una cultura al interior de la empresa orientada a la seguridad, admite aumentar un esquema de control de una forma más interactiva, rápida y eficiente en cuanto a las tareas o actividades a la que se dedica la empresa y así tener un mejor control de los recursos e información que allí se maneje.

Existen, en los tiempos que transitan, dos elementos que aumentan la importancia de brindar una adecuada seguridad a la información por parte de las empresas: la importancia creciente de la información para las empresas y le aumento de los riesgos a la que la misma se ve expuesta.

Para nadie es un secreto que estas entidades manejan grandes cantidades de información, las cuales le generan a estas entidades el posicionamiento y valor económico en el mercado por el cual compiten. Para cualquier individuo con conocimientos informáticos es un gran reto violar el esquema de seguridad informática de una empresa con reconocimiento y líder en el mercado ya que esto bajaría enormemente sus activos además de crear desconfianza e incomodidad con sus clientes.

Estas organizaciones pueden llegar a arrollar o caer solamente por la información que manejan, lo que ha llevado a que estas sean consideradas un activo cada vez más valioso, aun cuando no podemos llegar a cuantificarla adecuadamente. Y es esto último lo que impide que la información se vea reflejada en una línea del balance general como si fuera un dato más.

2.1.3 RIESGOS DE HACKING EMPRESARIAL

La Información es un activo que como cualquier otro activo importante de un negocio, tiene valor para las empresas, consecuentemente necesita ser salvaguardada de manera adecuada.

Antes de seguir hablando de este tema… quisiera preguntarte a ti… ¿crees tú que existen empresas con sistemas operativos, aplicaciones y configuración de los sistemas totalmente seguras?....¿ considera usted que los compañeros de trabajo, administrativos y personal de planta de sus empresa tienen pleno conocimiento sobre amenazas y vulnerabilidades de los sistemas informáticos?. Por consiguiente, por vulnerabilidad entendemos la exposición latente a un riesgo.

En el área de informática, existen varios riesgos tales como: 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.[15]

Pues bien, 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.

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

Específicamente, en los ataques de negación de servicio, el equipo de cómputo ya no es un blanco, es el medio a través del cual es posible afectar todo el entorno de red; es decir, anular los servicios de la red, saturar el ancho de banda o alterar el Web Site de la compañía. Con ello, es evidente que los riesgos están en la red, no en la PC.

Es por la existencia de un número importante de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo.[16]

Es por esto, que toda organización debe estar en alerta y saber implementar sistemas de seguridad basados en un análisis de riesgos para evitar o minimizar las consecuencias no deseadas. 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 clave de negocio más críticos y vinculados al logro de los objetivos de la empresa.

2.1.4 QUE ES EL ANÁLISIS DE RIESGOS

Es un paso importante para implementar la seguridad de la información. Como su propio nombre lo indica, es realizado para detectar los riesgos a los cuales están sometidos los activos de una organización, es decir, para saber cuál es la probabilidad de que las amenazas se concreten.

[16] Ibíd.

Las amenazas se pueden convertir en realidad a través de fallas de seguridad, que conocemos como vulnerabilidades y que deben ser eliminadas al máximo para que el ambiente que se desea 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 corrección de los activos que se desean proteger y deben ser siempre considerados cuando se realiza un análisis de riesgos.

AMENAZA

Aprovechan las vulnerabilidades encontradas en nuestros sistemas y que se convierten en:

Que originan

INCIDENTES

Son los hechos que **deben ser evitados**en una organización,puesto que causan impacto alos negocios.En virtud de la acción de unagente o condición natural, que son las amenazas en sí mismas, los incidentes generan una serie de problemas que pueden afectar los principios dc la seguridad dc la información

IMPACTOS

Los impactos pueden ser desastrosos, según su **amplitud y gravedad**. Sin importar el tipo de incidente, lo importante es **evaluar el impacto que Pucdc causar**en los diferentes activos de la empresa.

Figura 2. Esquema de relación de la amenaza incidente impacto

La figura 2 se muestra paso a paso la relación que hay entre amenaza-incidente-impacto. En consecuencia con lo planteado anteriormente revisaremos un ejemplo específico de la relación entre los conceptos de amenaza, incidente e impacto.

2.1.5 EJEMPLO DE LA RELACIÓN AMENAZA-INCIDENTE-IMPACTO

Empecemos con el caso de la pérdida de un documento confidencial, que trae el listado de los principales deudores de una empresa. El incidente de la pérdida de esta información en sí es pequeño, pero el impacto que puede causar es inmenso, cuando se divulguen los nombres de las personas deudoras.

En el caso de la acción de una amenaza de un fenómeno meteorológico como un huracán, el incidente puede ser muy grande, pero si la empresa cuenta con la protección adecuada en su infraestructura, el impacto puede ser pequeño.

Como podrá darse cuenta, con lo que se hemos comentado, sólo se hace referencia a lo que usted ya sabe, la tecnología es clave para su negocio, y con el incremento en frecuencia de los ataques a los mismos, su seguridad se convierte en algo vital para la supervivencia de la empresa.

> Una actividad centrada en la identificación de fallas de seguridad que evidencien vulnerabilidades que puedan ser explotadas por amenazas, provocando impactos en los negocios de una empresa. También podemos definir lo como una actividad de análisis que pretende, a través del rastreo,

identificar los riesgos a los cuales los activos se encuentran expuestos y tiene por resultado:

- ❖ Encontrar la consolidación de las vulnerabilidades para identificar los pasos a seguir para su corrección.
- ❖ Identificar las amenazas que pueden explotar esas vulnerabilidades y de esta manera se puede llegar a su corrección o eliminación.
- ❖ Identificar los impactos potenciales que pudieran tener los incidentes y de esta forma aprovechar las vulnerabilidades
- ❖ Determinar las recomendaciones para que las amenazas sean corregidas o reducidas.[17]

Otro punto importante a razonar en la realización del análisis de riesgos es la reciprocidad costo-beneficio. Este cálculo consiente que sean evaluadas las medidas de seguridad con relación a su aplicabilidad y el beneficio que se incrementará al negocio. 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.

[17] http://www.piramidedigital.com/Documentos/ICT/pdictsegurindadinformaticariesgos.pdf

2.1.5.1 ¿CUÁLES SON LOS PASOS QUE DEBEN DAR LAS EMPRESAS PARA IMPLEMENTAR LA SEGURIDAD INFORMÁTICA?

Lo primero es identificar el riesgo. Conociendo el riesgo al que se exponen les resulta más fácil aplicar soluciones de seguridad. Si no se conoce, difícilmente se sabrá qué mecanismos se deben aplicar. Entonces, lo primero que recomendamos es hacer un análisis de riesgos y ordenarlos según su prioridad.

Dependerá de la prioridad y de los recursos que requieran el que los riesgos sean mitigados, eliminados o asumidos, en caso que el impacto no sea mayor. Siempre hay una franja en la cual tengo un riesgo que es inaceptable, un riesgo aceptable, y trato de llegar a una franja en el medio, que es la "administración de riesgo".[18]

2.1.5.2 ¿CUÁLES SON ESOS RIESGOS QUE AFECTAN A LAS EMPRESAS Y ANTE LOS CUALES DEBERÍAN MANTENERSE ALERTAS?

Hay todo tipo de riesgos desde el punto de vista tecnológico y otros que no son tecnológicos. Un riesgo tecnológico, por ejemplo, es no tener bien configurado un servidor para tener passwordseguras. En muchos casos el servidor acepta una contraseña que sea simplemente 123. Si yo configuro el servidor de manera tal que me exija una contraseña que incluya números, letras y símbolos, estoy automáticamente mejorando la seguridad. El riesgo es que si no tengo passwordcomplejas cualquiera puede acceder a documentos, información confidencial o al correo electrónico.[19]

[18] http://www.mundoenlinea.cl/noticia.php?noticia_id=754&categoria_id=4
[19] Ibíd.

2.1.5.3 MOMENTO DE ANÁLISIS DE RIESGOS

El análisis de riesgos puede ocurrir antes o después de la definición de una política de seguridad. Según la norma internacional BS/ISO/IEC 17799, esta actividad puede ser hecha después de la definición de la política.

El propósito de tomar en cuenta una política de seguridad en el análisis se debe a varias razones:

- La política de seguridad delimita el alcance del análisis.
- Permite ser selectivo en la verificación de activos que la política establece como vulnerables.
- El análisis toma en cuenta la lista de amenazas potenciales que la misma política contempla.

Para tener más claro por qué decimos que la definición de una política de calidad marca el momento para iniciar un análisis de riesgos de la seguridad de la información recordemos qué es política de seguridad:

1. Es una medida que busca establecer los estándares de seguridad a ser seguidos por todos los involucrados con el uso y mantenimiento de los activos.

2. Es una forma de suministrar un conjunto de normas internas para guiar la acción de las personas en la realización de sus trabajos. Es el primer paso para aumentar la conciencia de la seguridad de las personas, pues está orientada hacia la formación de hábitos, por medio de manuales de instrucción y procedimientos operativos.

Sin embargo, la realización del análisis de riesgos como primer elemento de la acción de seguridad, es un hecho determinante para procesos críticos en que son analizadas todas las amenazas. De esta manera son considerados y analizados todos los activos de la organización, sea por muestreo o en su totalidad, para que estén libres de vulnerabilidades con el propósito de reducir los riesgos.

Por esta razón serán abordados en esta unidad todos los elementos necesarios para la realización de un análisis de riesgos como etapa de rastreo de vulnerabilidades de todo el ambiente de un proceso de negocios.

Algunos factores que pueden ser considerados y que tienen influyen en el momento de la realización de un análisis de riesgos son los siguientes:

Factores	Acción
Valor alto o alta exposición de los bienes afectados	Disminuir margen de tiempo
Históricamente los bienes atacados son afectados	Disminuir margen de tiempo
Factores atenuadores en acción	Aumentar margen de tiempo
Bajo Riesgo de exposición para los bienes afectados.	Aumentar margen de tiempo

Tabla 1. Factores que tienen gran influencia al momento de realizar un análisis de riesgo.

En la tabla 1 se muestra cuáles son los factores y acciones que se deben evaluar al momento de realizar un análisis de riesgo. Además de identificar el momento del análisis antes o después de la definición de una política de seguridad, existe otra serie de factores que determinan la oportunidad de ese análisis. Esta tabla ilustra la manera en que el tiempo tomado para la realización del análisis de riesgos debe ser afectado en razón de algunos de esos factores.

Como se observa en la imagen, entre mayor sea la exposición o el daño histórico a los bienes de la empresa, el margen de tiempo tomado para el análisis de riesgos debe ser menor y viceversa. Para tener más clara esta relación revisemos unos ejemplos concretos de cada uno de los factores:

Factores	Acciones
Valor alto o alta exposición de los bienes Afectados	En una empresa de asesores en contabilidad, los activos comúnmente afectados son las bases de datos con las auditorias de sus clientes, y por tanto, son de alto valor para la compañía y sus negocios.
Históricamente los bienes atacados son Afectados	En una empresa se tienen estadísticas de que los servidores que han sido atacados por virus o hackers siempre resultan dañados en su información o configuración y esto ocasiona perjuicios en las operaciones de la compañía.
Factores atenuadores	Si por ejemplo, sabemos que los activos que comúnmente son atacados en la empresa no poseen un alto valor para los negocios de la misma
Bajo Riesgo	Los activos que comúnmente en la empresa se catalogan como de bajo riesgo son por citar alguno, las estaciones de trabajo que no manejan o almacenan información vital para los negocios.

Tabla 2. Ejemplo de un análisis de riesgo.

La tabla 2, nos muestra un ejemplo más claro y aterrizado de lo que es una análisis de riesgo. Además de conocer el momento y duración adecuada para la realización de nuestro análisis de riesgos. También nos permite observar los diferentes ámbitos en los que podemos aplicar dicho análisis. La presente sección tiene como propósito presentar a usted dichos ámbitos.

En actualidad las de riesgos pueden formarse en distintos ámbitos. Por lo general, todos son considerados, puesto que la implementación de seguridad que pretende corregir el entorno en que se encuentra la información, es decir en actividades relacionadas a:Generación, Tránsito, Procesamiento,

Los riesgos pueden evaluarse según el impacto que este genere a las empresas en: alto, medio y bajo. Ya que de alguna manera siempre se ve afectada la entidad y de acuerdo al área en la que se encuentre la vulnerabilidad se denomina el ámbito.

2.1.6 RELACIÓN ENTRE LOS RIESGOS Y ÁMBITOS DEL ANÁLISIS DE RIESGOS

AMBITO	IMPACTO DE LOS RIESGOS			ASPECTOS POR ANALIZAR	DESCRIPCIÓN
	BAJO	MEDIO	ALTO		
TECNOLOGICO			Los servidores de ficheros, en los que se encuentran la información sobre el servicio o producto. Un servidor de datos que almacena la información de los clientes del Internet. Un servidor de correo electrónico (para envío de estado de cuenta por correo electrónico) un servidor Web. firewall, ruteador, parámetro, conexión, puente. Los servidores de ficheros, en los que se encuentran la información sobre el servicio o producto.	El análisis de riesgos realizado en el entorno tecnológico pretende el conocimiento de las configuraciones y de la disposición topológica de los activos de tecnología que componen toda la infraestructura de respaldo de la información para comunicación, procesamiento, tránsito y almacenamiento.	aplicación y equipo, sin dejar de considerar también la sensibilidad de las informaciones que son manipulados por ellos. Los usuarios que los utilizan. La infraestructura que les ofrece respaldo.
HUMANO	Personas que usan el Internet. Quienes dan soporte a los usuarios o administran los activos de la empresa. Responsable de la planeación y organización de los trabajos.	Las personas que trabajan como equipos en la definición de las políticas y procedimientos para la realización del proceso de empresa.	Es posible detectar cuáles vulnerabilidades provenientes de acciones humanas, se encuentran sometidos los activos, y es posible dirigir recomendaciones para mejorar la seguridad en el trabajo humano y garantizar la continuidad de los negocios de la organización.	El análisis de riesgos también se destina a la comprensión de las maneras en que las personas se relacionan con los activos. Así, es posible detectar cuáles vulnerabilidades provenientes de acciones humanas, se encuentran sometidos los activos, y es posible dirigir recomendaciones para mejorar la seguridad en el trabajo humano y garantizar la continuidad de los negocios de la organización. Este análisis pretende inicialmente identificar vulnerabilidades en los activos de tipo usuario y organización.	nivel de acceso que las personas tienen en la red o en las aplicaciones. Las restricciones y permisos que deben tener para realizar sus tareas con los activos. El nivel de capacitación y formación educativa que necesitan tener acceso para manipularlos.
PROCESO			El flujo de actividades relacionadas a la atención a los clientes. El flujo necesario de información para la realización de transacción.	Análisis de los flujos de información de la organización y la manera en que la información transita de un área a otra, cómo son administrados los recursos en relación a la organización y manutención. De esta manera, será posible identificar los eslabones entre las actividades y los insumos necesarios para su realización con el objetivo de identificar las vulnerabilidades que puedan afectar la confidencialidad, la disponibilidad y la integridad de la información y en consecuencia, del negocio de la organización. En este ámbito, el activo de enfoque principal es del tipo usuario e información.	Identificar a las personas involucradas en el flujo de información, es posible evaluar la necesidad real de acceso que ellas tienen a los activos. Evaluar el impacto proveniente del uso indebido de la información por personas no calificadas.
FÍSICO		Los locales de trabajo de los equipos involucrados, las agencias o puestos de atención al cliente.	Los locales de almacenamiento de la información crítica. Las centrales de proceso de información como los centros de proceso de datos, las salas de servidores, las centrales de procesamientos por teléfono, la sala caja fuerte.	Los locales de almacenamiento de la información crítica. Las centrales de proceso de información como los centros de proceso de datos, las salas de servidores, las centrales de procesamientos por teléfono, la sala caja fuerte.	Identificar posibles fallas en la localización física de los activos tecnológicos. Evaluar el impacto de accesos indebidos a las áreas en donde se encuentran activos tecnológicos. Evaluar el impacto de desastres ambientales en la infraestructura de tecnología de la empresa.

Tabla 3 relación entre riesgo y ámbito

La tabla 3, describe la relación que hay entre ámbito y riesgos en cuanto a la seguridad informática y que tan alto es el riesgos que se toma en cada una de las decisiones con respecto a los diferentes ámbitos.

2.1.6.1 HISTORIA DEL HACKING ETICO

El nombre hacker viene de un neologismo utilizado para referirse a un experto (Gurú) en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes, sistemas operativos.[20]

Estas personas con conocimientos previos en tecnología gozaban aportando sus ideas a las organizaciones donde trabajaban. Pero con el pasar del tiempo estos fueron cambiando la mentalidad de ayudar a las empresa donde se desempeñan como trabajadores en el área tecnológica; otros ex empleado de la empresa que tomaron represaría dieron lugar a lo que hoy se conoce como cracker.

El "Cracker (criminal hacker, 1985). Un cracker es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo."[21]

[20] http://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_0.pdf
[21] Ibíd.

2.1.6.2 QUE ES EL HACKING ETICO EMPRESARIAL

No es más que profesionales contratados dentro de las organizaciones para que emulen metodologías utilizadas por intruso con el fin de encontrar falencias en su seguridad. Los profesionales de la seguridad, que aplican sus conocimientos de hacking lo que buscan es defender los recursos informáticos y privilegiados dentro de las organizaciones de forma legal y sin poner en riesgo ningún tipo de información que suspenda las actividades a la que se dedica la empresa.

“Sí, en cambio, diremos que la ética implica que el trabajo y la intervención del profesional en seguridad informática o de la información no comprometen de ningún modo los activos de la organización, que son los va liosos datos con los que ella cuenta.

Estos daños podrían ser hechos de varias maneras: alteración, modificando a conciencia registros o datos sensibles; borrado, destruyendo información, bases de datos o sobrescribiendo algún tipo de dato; dar a conocer información a ter ce ros, incumpliendo las normas de confidencialidad; sustracción, roban do o guardando datos en medios de almacenamiento externos.

Todo esto, ya sea en la búsqueda de riesgos mediante un security assessment o comprobación de seguridad, como también en la divulgación de lo que se vio, habló, escuchó o manipuló en el transcurso, en la planificación o en el desarrollo de la tarea misma y en su análisis final.

Más allá de la ética propia de cada profesional, existen conductas mínimas que éste debe cumplir: Hacer su trabajo de la mejor manera posible, dar el mejor reporte, acordar un precio justo, respetar el secreto, no hablar mal ni inculpar a un administrador o equipo de programadores, no aceptar sobornos, no manipular o

alterar resultados o análisis, delegar tareas específicas en alguien más capacitado, no prometer algo imposible de cumplir, ser responsable en su rol y función, manejar los recursos de modo eficiente."[22]

Los elementos que mas importantes que se deben mantener en la seguridad son: confidencialidad la cual tiene que ver con el ocultamiento de información o recursos, autenticidad que es la identificación y garantías del origen de la información o recursos, integridad la cual se refiere a cambios no autorizados en los datos y por último disponibilidad la cual se refiere a la posibilidad de hacer el uso de la información y recursos deseados.

Este tema ha dado pie a que se incorporen otros términos dentro de él como es el Hacktivismo, el cual se refiere a hackear por una causa como es el caso de Anonymous. Además podemos decir que es el compromiso político o social del hacking.

En actualidad, atacar y alterar sitios web por razones políticas, tales como ataques a sitios web del gobierno o de grupos que se oponen a su ideología, son considerados acciones delictivas tengan o no tengan una justificación ideológica.

[22] Hacking Etico - Carlos Tori – 2008 http://www.4shared.com/get/yxDJ4VYZ/Hacking_Etico_-_Carlos_Tori.html

3 DEFINICION Y COMPARACION DE TECNICAS DE HACKING

Del conocimiento que se adquiera acerca de las herramientas de ataque, depende en gran medida la solución a implementar dentro de los sistemas informáticos en una organización.A continuación se presenta una clasificación de las diferentes formas de ataque, una evaluación de las posibles consecuencias que derivan de éstos, así como las maneras más acertadas de prevenirlos y contrarrestarlos.

3.1 MONITORIZACION

Básicamente es un conjunto de métodos de ataque que comprenden unas etapas de observación, donde se analizan las vulnerabilidades de la víctima y un posible acceso.

3.1.1 SCANNING (ESCANEO DE PUERTOS)

El Escaneo de puertos es el precursor de muchas intrusiones y ataques. En ausencia de información privilegiadao de información pública sobre una red de destino, estas exploraciones son el primer paso en la obtención deinformación básica sobre la red.

3.1.1.1 OBJETIVO DEL ATAQUE

Indagar por el estado de los puertos de un host conectado a una red, y si éstos puertos están abiertos analizar posibles vulnerabilidades.

3.1.1.2 MODO OPERACIONAL

Lo que se busca con esta técnica de hacking básicamente es observar cuáles puertos están abiertos ó cerrados. También se puede corroborar si existe algún tipo de firewall en la máquina ó en la red.

Esta técnica se subdivide en algunas prácticas que han sido implementadas de acuerdo con ciertos elementos ó factores como son clases de protocolos, puertos en escucha, y hasta el tipo de sistema operativo. Estas son:

> TCP connect: Forma básica de escaneo de puertos. Se intenta establecer conexión con varios puertos de la máquina objetivo. Si el puerto está escuchando,devolverá una respuesta de éxito y se establece la conexión. Cualquier otro evento significará que el puerto está cerrado.Esta técnica se caracteriza por ser rápida y no precisar ningún permiso de usuario sobre la máquina víctima. Sin embargo, es una técnica que se detecta fácilmente ya que los intentos de conexión queda registrados en la máquina objetivo.[23]
>
> TCP SYN: Este escaneo usa la técnica de “la media apertura”. Consiste en mandar un paquete TCP SYN al puerto objetivo. Si este

[23] Sistema híbrido para la detección de código malicioso - Jorge Argente Ferrero - 2.009

puerto está abierto contestará con un paquete ACK y si no es así responderá con un paquete RST. Si el puerto está abierto se responderá al paquete ACK con un paquete RST para no establecer la conexión y no dejar rastro en la máquina objetivo.Es una técnica poco ruidosa y muy sutil ya que no se llega a establecer conexión en ningún momento.[24]

TCP FIN: Consiste en el envío de un paquete FIN a un puerto. Si éste responde con un RST el puerto estará cerrado. Sin embargo, si no se obtiene ninguna respuesta significa que el puerto está abierto.Esta técnica es la más efectiva para no ser detectados, sin embargo sólo funciona en sistemas LINUX/UNIX ya que en Windows siempre responde con un RST a los paquetes FIN.[25]

Escaneo fragmentado:Este procedimiento consiste en fragmentar los paquetes de sondeo dirigidos a la máquina víctima. Con esto conseguimos provocar menos ruido en las herramientas de protección (firewalls) del sistema objetivo.[26]

3.1.1.3 CONSECUENCIAS

- Constantes avisos del firewall.
- Utilización maliciosa de puertos abiertos por parte de intrusos.

[24] Ibíd
[25] Ibíd
[26] Ibíd

3.1.1.4 CÓMO DETECTAR EL SCANNING?

> La detección de estos escaneos iniciales puede permitir a los defensores bloquear posibles atacantes antes de que puedan ser peligrosos. Sin embargo, los análisis en los puertos son aleatorios y rápidos y los métodos de detección de Escaneo no son tan eficientes para detectarlos y predecirlos.[27]

Al descubrir un escaneo de puertos el siguiente paso es no acceder ó permitir los intentos de conexión de la máquina que realiza el escaneo, ya que lo que intenta es obtener información del sistema que ataca.

Es de suma importancia que todo esté bien configurado. También es importante una aplicación que cubra todos los requerimientos y con unos buenos estándares de encriptación que aseguren la información, y un firewall que garantice el cuidado de los puertos (cuándo abrirlos y cerrarlos). Una práctica aconsejable dentro de las empresas es realizar, periódicamente, escáneres a la propia organización para ver cómo está en materia de seguridad informática.

3.1.2 ENUMERACIÓN DEL OBJETIVO

Este es uno de los principales pasos de cualquier ataque de hacking, aunque en sí mismo no represente peligro inminente. Con esta técnica se recoge y organiza la mayor cantidad de información atinente a computadores, redes, aplicaciones y servicios. Al tener toda esta información organizada y disponible a la hora de consultar, lo que se pretende es avanzar a un siguiente estado donde el ataque cobra fuerza y los resultados van a ser inmediatos.

[27] Detecting stealthy scans and scanning patterns using threshold random walk - Vagishwari S. Nagaonkar - 2008

3.1.2.1 OBJETIVO DEL ATAQUE

El objetivo principal es obtener la mayor cantidad de información sensible que servirá para un ataque futuro

3.1.2.2 MODO OPERACIONAL

Se establecen conexiones activas con el sistema y se llevan a cabo consultas dirigidas. Se puede obtener información en lo que respecta a máquinas, recursos de red, aplicaciones, y hasta información referente al sistema operativo. También se recolectan datos sobre los recursos del sistemaque se encuentren mal configurados y vulnerabilidades del sistema que se tiene por objetivo.

Casi siempre los datos que se obtienen con esta herramienta es información pública, como direcciones de DNS.

3.1.2.3 CONSECUENCIAS

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.

3.1.2.4 MEDIDAS DE PREVENCIÓN

Estos son algunos consejos para protegerse de ataques de enumeración:

- Corregir los protocolos que contestan de diferente modo si el usuario existe o no.
- Configurar correctamente los servicios para que no muestren más información de la necesaria.
- No usar nombres por defecto para archivos de configuración.
- Desactivar puertos de administración http y snmp.
- Cambiar el password por defecto de todos los lugares.[28]

3.1.3 SNIFFING (OLFATEO)

También llamada “Robo de información”. Con esta técnica “se escucha la información cuando esta no va dirigida a lamáquina que está capturando el tráfico”[29].

3.1.3.1 OBJETIVO DEL ATAQUE

Obtener información de todo el tráfico que pasa por una red, no importa si los datos están encriptados.

[28] Seguridad en VoIP: Ataques, Amenazas y Riesgos - Roberto Gutiérrez Gil -2008

[29] Seguridad Informática: Técnicas hacker - Jesús Moreno León - 2010

3.1.3.2 MODO OPERACIONAL:

En esta técnica “se usan analizadores de protocolos (packetsniffers), que sonprogramas que permiten monitorizar y analizar el tráfico de unared”[30].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.

Un sniffer es un programa que trabaja dentro de la red en conjunto con la tarjeta de interfaz de red (NIC, Network Interface Card), para atraer todo el tráfico que está a su alcance, incluso más allá de los routers y dispositivos similares.

Para llevara cabo el Sniffing existen un conjunto de aplicaciones, y entre ellas las principales son:SpyNet, Ethereal, WinSniffer

3.1.3.3 CONSECUENCIAS:

Al detectar toda la información que circula por la red se ponen en evidencia elementos confidenciales tales como números de tarjetas de crédito, nombres y contraseñas de usuarios y más información sensible.

[30] Ibíd

3.1.3.4 CÓMO PREVENIRLA Y/O DETECTARLA

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.

Hay que resaltar la importancia que cobra el hecho de enviar la información de manera encriptada con algún tipo de tecnología de encriptación como lo son PGP ó GnuPG.Para evitar ataques en las redes se recomienda utilizar encriptación WPA, debido a que la protección WEP es demasiado vulnerable al software Sniffer. Si sólo se cuenta con WEP, la contraseña debe ser cambiada con regularidad. Por otra parte, los routers deben estar bien protegidos con contraseñas.

3.2 VALIDACION

Este tipo de técnicas tienen como objetivo el suplantar al dueño o usuario de la máquina mediante el uso de sus cuentan de acceso y contraseñas.[31]

3.2.1 FUERZA BRUTA

El ataque por fuerza bruta se define como el procedimiento por medio del cual se intenta acceder por medio de la obtención de la clave.Los tipos de ataque por fuerza bruta son:Objetivo ataque, Trawlingattack, A ciegas

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

3.2.1.1 OBJETIVO DEL ATAQUE

Generar claves (mediante la combinación secuencial de caracteres) y probarlas en determinado servicio de autentificación o archivo para verificar sicoinciden con un login válido de acceso (usuario y clave o sólo clave).[32]

El objetivo del hacker ético es verificar la vulnerabilidad de lo que debe proteger y solucionarla.[33]

3.2.1.2 MODO OPERACIONAL

En el objetivo ataque, el atacante trata de adivinar utilizando algún tipode estrategia de la fuerza bruta, el valor, por ejemplo, de la contraseñaque autentica a un usuario determinado. En este caso, el éxito del ataque depende de la fortaleza de la contraseña utilizada en la cuenta atacada.[34]

En este tipo de ataque, donde se recibe un sin número de intentos de acceso, es común encontrar cierto nivel de defensa.

[32] Hacking Etico - Carlos Tori - 2008
[33] Ibid
[34] Lightweight protection against brute force login attacks on web applications - http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=5593241

> En el segundo tipo de ataque, el atacante elige una contraseña y trata de encontrar una cuenta de usuarioque utiliza esta contraseña. Es exitoso si el espacio de nombres utilizados parael identificador de la cuenta es conocido o fácil de adivinar.[35]

En el último tipo de ataque por fuerza bruta, se busca tanto el nombre de la cuenta como la contraseña al mismo tiempo.

Los ataques por fuerza bruta se realizan, en gran medida, obteniendo el archivo donde están todas las contraseñas encriptadas, y de manera offline se pueden hallar todas las combinaciones posibles de dichas contraseñas. Cuando una contraseña tiene cinco dígitos existen cien combinaciones posibles.

Algunos sistemas no permiten acceder cuando se ha incurrido en cierto número de intentos fallidos. Sin embargo algunos le hacen la vida fácil a quienes pretenden acceder con esta técnica, ya que utilizan las contraseñas más comunes como por ejemplo su fecha de nacimiento, número de teléfono oincluso hasta su nombre.

> En septiembre de 2009, un total de 9.843 contraseñas se filtrarondesde el servicio de correo electrónico de Hotmail. La contraseña más común eneste conjunto fue "123456", y se utilizó por el 0,65% de los usuarios.[36]

[35] Ibíd
[36] Ibíd

3.2.1.3 MEDIDAS DE DEFENSA

Las medidas para defenderse contra los ataques por fuerza bruta permiten de cierta manera controlar el intento de acceso no autorizado pero no son el remedio que todos esperan.

> El más común de estos mecanismos es el denominado "regla de los tres strikes", que consiste enel bloqueo del acceso a una cuenta después de varios intentos de inicio de sesión fallidos (generalmente tres). El problema obvio con estemecanismo es que al tener un número tan bajo de intentos, los mismos usuarios legítimos pueden bloquearsu propia cuenta. El uso de un mayor número deintentos antes de bloquear la cuenta, por ejemplo, 20 ó 30 intentos,sería mucho más fácil de usar y no impactaría, de manera significativa,la seguridad del sistema.[37]

Otro mecanismo muy utilizado es aquel que deshabilita temporalmente la cuenta, y a veces esto se hace entre dos intentos de inicio de sesión. Algunas empresas, en su afán de contrarrestar el robo de sus contraseñas, tienen como política el cambio de contraseñas cada cierto período de tiempo.

3.2.2 SPOOFING (SUPLANTACIÓN)

El Spoofing es un tipo de técnica de camuflaje online donde se suplanta la identidad de un dispositivo en una red informática para obtener información

[37] Ibíd

restringida. Este ataque tiene algunas variedades entre las que se destacan el IP Spoofing (enmascaramiento de la dirección IP), que es el genérico y que “consiste en generar paquetes de información con una dirección IP falsa”[38], y por ende, falsificar la cabecera de los paquetes enviados a un determinado sistema informático, donde el paquete pareciera que viene de otra persona. Con esto, la persona que realiza el ataque selecciona una dirección IP que pertenece a un equipo legítimo y así puede acceder a cualquier otro sistema.

Las distintas técnicas de Spoofing se basan en los protocolosARP (protocolo de resolución de direcciones), ICMP (protocolo de mensajes de control de Internet), RARP (protocolo de resolución de direcciones inversa).

3.2.2.1 OBJETIVO DEL ATAQUE

En relación a que son diversos los ataques con Spoofing, también varían los objetivos en estos tipos de ataques. Entre ellos tenemos:

- Falsificar datos.
- Adquirir información de una determinada máquina
- Simular la identidad de otro

3.2.2.2 MODO OPERACIONAL IP SPOOFING

Esta variedad de Spoofing tiene ciertas desventajas iniciales, como es el hecho de que el host víctima puede cortar la conexión o que los

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

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.[39]

Otro tipo de Spoofing es el DNS Spoofing**;** también llamado Pharming. Se trata del cambio de la relación de un nombre de un dominio por una IP falsa. Este ataque se realiza si el servidor DNS no es muy seguro, ó si confía en otros que sí son inseguros. Por otro lado, una vez se haya realizado el cambio, otros servidores DNS que se fíen de este, podrán añadir a sus cachés la dirección falsa, denominándose DNS poisoning.[40]

Después del ataque pueden ocurrir algunos escenarios como que el software descargado de internet sea de sitios que no son legítimos, es decir programas maliciosos.

3.2.2.3 MODO OPERACIONAL DE ARP SPOOFING

El ARP Spoofing introduce una dirección IP falsa a la asignación de direcciones MAC en la tabla ARP. El envenenamiento ARP se puede hacermediante la actualización de una entrada ARP existente.[41]

Lo que se busca con esta técnica es que la víctima envíe los paquetes al destino del atacante en lugar de remitirlos al destino legítimo.

---

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

[40] Ibíd

[41] A Host Based DES Approach for Detecting ARP Spoofing - http://ieeexplore.ieee.org.ezproxy.utp.edu.co/search/srchabstract.jsp?tp=&arnumber=5949401

3.2.2.4 CONSECUENCIAS

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

3.2.2.5 MEDIDAS DE DEFENSA IP SPOOFING

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.

3.2.2.6 CÓMO EVITAR EL ARP SPOOFING

Existen dos casos. Para una red pequeña la utilización tanto de IP estáticas como tablas ARP estáticas puede ser la solución. Para otro tipo de redes la solución debe estar asociada a la dirección MAC y cómo impedir que ésta pueda ser modificada en los host; ya que si se piensa en la primera solución sería imposible actualizar las entradas de nuevas máquinas en la tabla ARP.

3.2.3 HIJACKING (ROBO DE SESIÓN)

El Hijacking es una técnica por medio de la cual se intercepta y se roba una sesión de algún usuario para apropiarsede algún servicio, después de que el usuario autorizado que se quiere suplantar se identifica ante el sistema remoto.

Los servicios de los que se apropia van desde módems, routers, las conexiones TCP/IP, dominios, páginas web e inicio de sesión.

3.2.3.1 OBJETIVO DEL ATAQUE

Secuestrar una conexión ya establecida de manera legal por otro usuario con un servidor.

3.2.3.2 CÓMO SE HACE

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 que ahora lo único que ve es como su conexión se ha colgado. A partir de este momento, el atacante tiene el control y continuará con su tarea de enviar datos.

3.2.3.3 CÓMO PROTEGERSE?

Como primera medida de protección se debe usar la encriptación, para que los datos que viajen por la red se encuentren codificados. Esto es fundamental ya que el Hijacking se basa en Sniffing que tiene como peor enemigo la información encriptada. Tampoco se puede dejar de lado el firewall, el antivirus, el antispyware y la utilización de programas como el Anti-Hijacker que tienen como finalidad resguardar las máquinas, las páginas webs, y hasta los módems de algún secuestro.

Los protocolos de seguridad tales como https son importantes también para evitar el robo de sesión y, por ende, de información.

3.2.4 INGENIERÍA SOCIAL

> La Ingeniería Social es un método basado en engaño y persuasión para obtener información significativa o lograr que la víctima realice un determinadoacto, como por ejemplo, ejecutar un archivo que le llegó por e-mail, que releve su contraseña por teléfono cuando se la solicitan o, por último, que esta persona incida sobre otra para enviar datos hacia un lugar determinado.[42]

3.2.4.1 OBJETIVO DEL ATAQUE

Obtener información y acceso a un sistema, por medio de personas, con el fin de irrumpir en la seguridad de éste.

[42] Hacking Etico - Carlos Tori - 2008

3.2.4.2 MODO OPERACIONAL

> Las personas, ya sea por ignorancia, negligencia o coacción, pueden permitir a un atacante obtener acceso no autorizado, quien, de esta manera, podrá eludir los complejos esquemas y tecnologías de seguridad que se hayan implementado en la organización. Por ejemplo, en este sentido, la confianza y la divulgación de información son dos de las debilidades más explotadas para obtener datos relacionados a un sistema.[43]

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”[44].

Las formas más comunes de usar ingeniería social son:

- El utilizado por algunos wormsmsn para lograr que nosotros hagamos click en determinado link que nos envía a través de un mensaje instantáneo, generado de forma automática. Con este fin, intenta hacernos creer que son fotos de amigos y así logra infectarnos, entre otras acciones.
- Los conocidos casos de Phishing en los que llega un supuesto e-mail de nuestro banco para que coloquemos nuestros datos personales. De esa manera, el delincuente los graba para finalmente extraer dinero de nuestra cuenta o vender los datos al mejor postor.

[43] Ataques informáticos. Debilidades de seguridad comúnmente explotadas - https://www.evilfingers.com/publications/white_AR.php
[44] Hacking Etico - Carlos Tori - 2008

- Las famosas postales electrónicas de invitación, saludos o amor enviadas por email que, al abrirlas, nos requieren que coloquemos nuevamente el login de nuestro correo electrónico, para ser grabado por el intruso y así poder acceder a nuestra cuenta.[45]

3.2.4.3 MEDIDAS DE PREVENCIÓN

Algunas medidas a tener en cuenta son:

- Nunca divulgar información sensible con desconocidos o en lugares públicos (como redes sociales, anuncios, páginas web, etc.).
- 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.
- Implementar un conjunto de políticas de seguridad en la organización que minimice las acciones de riesgo.
- Efectuar controles de seguridad física para reducir el peligro inherente a las personas.
- Realizar rutinariamente auditorías y pentest usando Ingeniería Social para detectar huecos de seguridad de esta naturaleza.
- Llevar a cabo programas de concientización sobre la seguridad de la información.[46]

Otra medida no menos importante es adquirir un servicio técnico propio ó de confianza, ya que por medio de éste le resulta fácil a cualquier persona extraer algún tipo de información.

[45] Ibíd

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

Pese a todo esto, la única manera de hacer frente a los métodos de Ingeniería Social es la educación. Absolutamente todas las personas que forman parte de la organización, desde la secretaria, los administradores de la red y la cúpula mayor, deben estar capacitados en cuanto a las debilidades y los métodos de engaño más empleados por los atacantes para que logren identificarlos y dar aviso de cualquier anomalía que se produzca en el equipo o en determinado ambiente. Esto no significa que cada uno de los empleados deba realizar cursos de seguridad informática, sino que el proceso de capacitación debe formar parte de las Políticas de Seguridad de la Información y debe ser ejecutada a través de planes dinámicos de concientización.[47]

3.3 D.O.S (DENEGACIÓN DE SERVICIO)

Técnica de ataquedonde se consigue que los servidores y redes informáticas colapsen y de esta manera ya no puedan brindar sus servicios como lo hacen habitualmente. Estos ataques pueden ser enviados desde uno o varios computadores. Cuando son enviados desde servidores, se denominan ataques distribuidos. A los servidores que cumplen con esta tarea se les conoce como zombies, y es el atacante quien se ha apropiado de ellos.

> Los ataques de denegación de servicio (DoS) no se limitan sólo a los sistemas finales. También incluyen routers de núcleo de red, switches y servidores de nombres de dominio.[48]

[47] Ataques informáticos. Debilidades de seguridad comúnmente explotadas - https://www.evilfingers.com/publications/white_AR.php

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

3.3.1 JAMMING (INTERFERENCIA)

Jamming se refiere al bloqueo de un canal de comunicación con la intención de impedir el flujo de información. Esta es una de las formas más temidas de los ataques en las redes inalámbricas. Esto es así porque, con la arquitectura de red existente, es muy poco lo que se puede hacer para superar un ataque de bloqueo.[49]

Son muy comunes las noticias de ataques D.o.S dentro de las entidades gubernamentales. En 2007, los sitios Web del Parlamento, los bancos y los organismos de radiodifusión en Estonia fueron víctimas de ataques de denegación de servicio. En 2008, numerosos sitios Web de Georgia fueron derribados por los ataques de denegación de servicio. En julio de 2009, un masivo ataque de denegación fue lanzado simultáneamente en muchos sitios Web de las organizaciones en Corea del Sur y Estados Unidos. Entre las víctimas (en los Estados Unidos) se tienen la Casa Blanca, el Servicio Secreto, Comisión Federal de Comercio, Departamento de Transporte, New York Stock Exchange, NASDAQ, YahooFinance y Washington Post. Se informó que los ataques fueron lanzados desde más de 20.000 zombies.[50]

[49] Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks - http://www.sciencedirect.com.ezproxy.utp.edu.co/science/article/pii/S0045790609000536

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

3.3.1.1 OBJETIVO DE JAMMING

El objetivo del ataque es inundar con pedidos falsos, saturando los recursos (disco duro, la memoria y el procesador) de las máquinas destino para que estos equipossean incapaces de proporcionar los servicios normales.

3.3.1.2 MODO DE OPERACIÓN

> 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; esto impide que oiga las solicitudes de otros usuarios que si necesitan la conexión.[51]
>
> En las redes inalámbricas los ataques de Jammingóbloqueo causan interferencias en las señales, lo que conduce a la congestión de la red. El resultado puede ser una interrupción total de los servicios.[52]
>
> Cuatro métodos de Jamming son:
> Constante: Envío aleatorio de bits de datos sobre un canal
> Engañoso: Envío de paquetes a un ritmo muy rápido
> Aleatorio: En este tipo de ataque se alterna entre dormir e interferir el canal de operación.

[51] Sistema hibrido para la detección de código malicioso - Jorge Argente Ferrero - 2.009
[52] Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks - http://www.sciencedirect.com.ezproxy.utp.edu.co/science/article/pii/S0045790609000536

Reactiva: Este tipo de bloqueo ataca sólo cuando escucha comunicación sobre el canal que está escaneando actualmente.[53]

3.3.1.3 MEDIDAS DE PREVENCIÓN

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.[54]

3.3.2 SYN FLOODING (ATAQUE POR SINCRONIZACIÓN)

Consiste 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.[55]

[53] Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks - http://www.sciencedirect.com.ezproxy.utp.edu.co/science/article/pii/S0045790609000536
[54] The dark side of the Internet: Attacks, costs and responses - http://www.sciencedirect.com.ezproxy.utp.edu.co/science/article/pii/S0306437910001328
[55] Sistema hibrido para la detección de código malicioso - Jorge Argente Ferrero - 2.009

3.3.2.1 MODO DE OPERACIÓN

Se inicia una sincronización de conexión con un servidor a un determinado servicio que proporcione.Posteriormente esta petición formará parte de la pila TCP/IP del servidor (ocupando desde aquí un espacio); luego el servidor esperará la respuesta del usuario (sobre aceptación de la conexión).El servidor puede esperar de 1 a 3 minutos a que el usuario responda; en caso que se sobrepase el tiempo, el servidor rechaza la conexión y libera el espacio de la pila. Mediante aplicaciones maliciosas o de auditoría de red, se pueden falsear (spoofear) las dirección IP de origen, haciendo múltiples intentos de conexión desde un mismo equipo, así mismo el servidor espera las respuestas de direcciones falseadas (spoofeadas). Esto realizado en mayor escala llega a saturar el ancho de banda y colapsar los servicios que brinda el servidor.[56]

3.3.2.2 OBJETIVO

Colapsar los recursos de las máquinas víctimas, excediendo el número de conexiones, para que no atiendan a usuarios legítimos.

3.3.2.3 CONSECUENCIAS

- Saturación de los recursos de memoria.
- Incapacidad de establecer conexiones adicionales.

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

- Inundación de puertos, como Smtp (correo electrónico) y http (contenido web) con conexiones.

Medidas:

- Blindar el servidor con un firewall del tipo stateful.
- Disponer de un sistema operativo actualizado.
- Habilitar la protección SYN Cookie

3.4 MODIFICACION

Este tipo de técnicas tienen como objetivo la modificación no autorizada de los datos y ficheros de un sistema. También pueden modificarse programas que se ejecutan en el sistema cambiando su funcionamiento.[57]

3.4.1 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.[58]

Se le llama “huellas” a todas aquellas tareas que ejecuta el atacante dentro del sistema. Estas tareas ó procedimientos son guardadas en archivos logs.

[57] Sistema híbrido para la detección de código malicioso - Jorge Argente Ferrero - 2.009
[58] Ibíd

3.4.1.1 OBJETIVO

El principal objetivo de esta técnica es ocultar todas las evidencias que pueden quedar al realizar cualquiera de los ataques antes descritos, pensando en que puede aprovechar la vulnerabilidad para realizar ataques futuros.

3.4.1.2 CÓMO SE HACE

> El intruso puede borrar sus rastros de muchas formas. La más grotescaes haciendo un simple rm –rf /var/log, ya que así podrían ser recuperados fácilmente con técnicas forenses simples. Diferente es si utiliza una herramienta de borrado seguro como Wipe, pero así se despiertan las sospechas del administrador. Puede hacerlo de manera más sutil si programa un zapper adecuado al objetivo y al modo de gestionar registros que existe en el servidor (que puede no estar por defecto). A su vez, debe borrar todos los logs que éste modifica tras su paso y sólo eliminar las entradas que corresponden a dichas sesiones.[59]

3.4.1.3 CONSECUENCIAS

- Posibilidad de ataque futuro, al no detectarse la intrusión a tiempo.
- Pérdida de información de la mano del borrado de archivos.

[59] Hacking Etico - Carlos Tori - 2008

3.4.1.4 MEDIDAS DE DETECCION

Es difícil guiarse por los logs después de una intrusión, ya que casi siempre han sido borrados. Pero 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 algo que, incluso, se puede llevar a cabo es el rastreo del atacante.

CUADRO COMPARATIVO Y CLASIFICACION DE LAS TECNICAS DE HACKING

Grupo	**Técnica**	**Definición**	**Objetivo del ataque**	**Modo operacional**	**Consecuencias**	**Cómo detectarla ó prevenirla**
Monitorización	Scanning	Primeras exploraciones para la obtención deinformación básica sobre la red de destino.	Indagar por el estado de los puertos de un host conectado a una red en busca de vulnerabilidades.	Se intenta establecer conexión con varios puertos de la máquina objetivo. En algunos casos se envían paquetes.	-Constantes avisos del firewall. - Utilización maliciosa de puertos abiertos.	-Con buenas configuraciones. - Con una aplicación que cubra todos los requerimientos. - Con buenos estándares de encriptación. - Con un firewall que garantice el cuidado de los puertos. - Se aconseja realizar, periódicamente, escáneres a la propia organización para ver cómo está en materia de seguridad informática.
	Enumeración	Técnica que pretenderecoger y organizar la mayor cantidad de	Obtener la mayor cantidad de información sensible que servirá para un	Establecimiento de conexiones activas con el sistema y	Con el conocimiento de cualquier sistema el intruso puede	-Corregir los protocolos que contestan de diferente modo si el usuario existe o

		información atinente a computadores, redes, aplicaciones y servicios.	ataque futuro.	realización de consultas dirigidas.	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.	no. - Configurar los servicios para que sólo muestren información necesaria. - No usar nombres por defecto para archivos de configuración. - Desactivar puertos de administración http y snmp. - Cambiar el password por defecto de todos los lugares.
	Sniffing	El Robo de información permite escuchar la información cuando esta no va dirigida a la máquina que está capturando el tráfico.	Obtener información de todo el tráfico que pasa por una red, no importa si los datos están encriptados.	Se usan analizadores de protocolos (packetsniffers), que permiten monitorizar y analizar el tráfico de una red. Estas aplicaciones descifran los paquetes de datos y los almacenan para luego analizarlos.	Al detectar toda la información que circula por la red se ponen en evidencia elementos confidenciales tales como números de tarjetas de crédito, nombres y contraseñas de usuarios y más información sensible.	- Enviar la información de manera encriptada. - Utilizar encriptación WPA en vez de WEP. - Proteger routers con contraseñas.
Validación	Fuerza bruta	Procedimiento por medio del cual se intenta acceder por medio de la obtención de la clave.	Generar claves y probarlas en determinado servicio de autentificación ó archivo para verificar si coinciden con un login válido de acceso.	Estos ataques se realizan, en gran medida, obteniendo el archivo donde están todas las contraseñas encriptadas, y de manera offline se hallan todas las combinaciones posibles de dichas contraseñas.	La principal consecuencia es que el intruso obtiene permisos sobre todo el sistema y puede infiltrarse fácilmente.	- Bloqueando el acceso a una cuenta después de varios intentos de inicio de sesión fallidos. - Deshabilitando temporalmente la cuenta cuando se realicen intentos de inicio de sesión fallidos. - Cambio de contraseñas cada cierto período de tiempo.
	Spoofing	Tipo de técnica de camuflaje	- Falsificar datos. - Adquirir	En el ARP Spoofingse introduce una	El riesgo más conocido es el de Phishing,	- Utilizando, tanto, IP estáticas como tablas ARP

		online donde se suplanta la identidad de un dispositivo en una red informática para obtener información restringida.	información de una determinada máquina - Simular la identidad de otro.	dirección IP falsa a la asignación de direcciones MAC en la tabla ARP. Con esto la víctima envía los paquetes al destino del atacante en lugar de remitirlos al destino legítimo.	donde una persona es timada y se le hace creer que ha entrado a su entidad financiera de confianza.	estáticas. - Impidiendo que la dirección MAC sea modificada en el host.
	Hijacking	Técnica de Hacking donde se intercepta y se roba una sesión de algún usuario para apropiarse de algún servicio.	Secuestrar una conexión ya establecida de manera legal por otro usuario con un servidor.	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 que ahora lo único que ve es como su conexión se ha colgado.	- Acceso no autorizado a información. - Corte de la conexión entre el usuario legítimo y el servidor.	- Usando encriptación, para que los datos que viajan por la red se encuentren codificados. - Utilizandofirewall, antivirus y antispyware. - Con protocolos de seguridad tales como https que son importantes para evitar el robo de sesión.
	Ingeniería Social	Método basado en engaño y persuasión, para obtener información significativa.	Obtener información y acceso a un sistema, por medio de personas, con el fin de irrumpir en la seguridad de éste.	Una de las maneras como opera es con supuestos emails del banco a su cliente (Phishing) donde éste debe poner datos personales. Así el delincuente los graba para finalmente extraer el dinero.	- Intromisiones a los sistemas y a las redes con información recolectada previamente. -Vulnerbilidad en redes, servidores, cuentas de usuario, … - Aquí también se da la modalidad de Phishing.	-Nunca divulgar información sensible con desconocidos ó en lugares públicos. - Si se sospecha que alguien intenta realizar un engaño, hay que exigir se identifique y tratar de revertir la situación intentando obtener la mayor cantidad de información del sospechoso. - Implementar políticas de

						seguridad. - Realizar programas de concientización sobre la seguridad de la información. - Adquirir un servicio técnico propio ó de confianza.
DoS	Jamming	Bloqueo de un canal de comunicación con la intención de impedir el flujo de información.	Inundar con pedidos falsos, saturando los recursos de las máquinas destino, para que estos equipos sean incapaces de proporcionar los servicios normales.	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; esto le impide que oiga las solicitudes de otros usuarios que sí necesitan la conexión.	- Saturación de los servidores. - Hacer una red inutilizable debido a la cantidad de tráfico.	- Eliminación de las vulnerabilidades conocidas en los comportamientos del protocolo y la configuración del host. - Filtrado del tráfico.
	SYN Flooding	Consiste 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	Colapsar los recursos de las máquinas víctimas, excediendo el número de conexiones, para que no atiendan a usuarios legítimos.	Mediante aplicaciones maliciosas se falsean las direcciones IP de origen, haciendo múltiples intentos de conexión desde un mismo equipo,	-Saturación de los recursos de memoria. - Incapacidad de establecer conexiones adicionales. - Inundación de puertos, como Smtp	- Blindando el servidor con un firewall del tipo stateful. - Disponiendo de un sistema operativo actualizado. - Habilitando la protección SYN

		tiempo para recibir la respuesta del atacante.		lo que al hacerse en mayor escala llega a saturar el ancho de banda y colapsar los servicios que brindan el servidor.	(correo electrónico) y http (contenido web) con conexiones.	Cookie.
Modificación	Borrado de huellas	Modificación de los ficheros log del sistema operativo de la máquina asaltada, para borrar el rastro dejado por el atacante.	Ocultar todas las evidencias que pueden quedar al realizar cualquier intrusión pensando en ataques futuros.	Programando un zapper adecuado al objetivo y al modo de gestionar registros que existe en el servidor. A su vez, borrando todos los logs que éste modifica tras su paso y sólo eliminando las entradas que corresponden a dichas sesiones.	- Posibilidad de ataque futuro, al no detectarse la intrusión a tiempo. - Pérdida de información de la mano del borrado de archivos.	Si se detecta la intrusión se pueden: -Cubrir los huecos de seguridad. - Evitar ataques posteriores. - Rastrear al atacante.

Tabla 4 definición y comparación de las técnicas de hacking

La tabla 4 muestra la relación que hay entre las distintas técnicas de ataques informáticos, que se pueden utilizar para violar a la seguridad de cualquier entidad.

4 APORTES

4.1 HACKING EMPRESARIAL

Conjunto de técnicas y procedimientos utilizados por una persona con gran cantidad de conocimiento en el ámbito de la contra informática; estas personas se

caracterizan por tres aspectos: la diversiónpor que se apasionan por lo que hacen de manera que cada día se enamoran más por lo que realiza. La otra es el talento que son Habilidad innata o capacidad de comprender y entender estos sistemas informáticos para extraer los recursos o información de forma adecuad. También se puede decir que es el potencial de un individuo para desempeñar muy bien actividades delictivas.

La exploración es la búsqueda continua de aquellas debilidades o fallas (parches, errores) en los sistemas. En los cuales estas personas ven la oportunidad de demostrar sus habilidades para cumplir un determinado objetivo. De esta manera, hacking significa explorar los límites de lo que es posible en un espíritu de traviesa inteligencia. Esta palabra suele asociarse a procedimientos ilegales o malignos.

4.2 RELACIÓN ENTRE LOS RIESGOS Y ÁMBITOS DEL ANÁLISIS DE RIESGOS

AMBITO	IMPACTO DE LOS RIESGOS			ASPECTOS POR ANALIZAR	DESCRIPCIÓN
	BAJO	MEDIO	ALTO		
TECNOLOGICO			Los servidores de ficheros, en los que se encuentran la información sobre el servicio o producto. Un servidor de datos que almacena la información de los clientes del Internet. Un servidor de correo electrónico (para envío de estado de cuenta por correo electrónico) Un servidor Web. firewall, ruteador, parámetro, conexión, puente. Los servidores de ficheros, en los que se encuentran la información sobre el servicio o producto.	El análisis de riesgos realizado en el entorno tecnológico pretende el conocimiento de las configuraciones y de la disposición topológica de los activos de tecnología que componen toda la infraestructura de respaldo de la información para comunicación, procesamiento, tránsito y almacenamiento.	aplicación y equipo, sin dejar de considerar también la sensibilidad de las informaciones que son manipulados por ellos. Los usuarios que los utilizan. La infraestructura que les ofrece respaldo.
HUMANO	Responsable de la planeación y organización de los trabajos. Las personas que trabajan como equipos en la definición de las políticas y procedimientos para la realización del proceso de empresa.	Personas que usan el Internet. Quienes dan soporte a los usuarios o administran los activos de la empresa.	El análisis de riesgos también se destina a la comprensión de las maneras en que las personas se relacionan con los activos. Así, es posible detectar cuáles vulnerabilidades provenientes de acciones humanas, se encuentran sometidos los activos, y es posible dirigir recomendaciones para mejorar la seguridad en el trabajo humano y garantizar la continuidad de los negocios de la organización.	El análisis de riesgos también se destina a la comprensión de las maneras en que las personas se relacionan con los activos. Así, este análisis pretende inicialmente identificar vulnerabilidades en los activos de tipo usuario y organización.	El nivel de acceso que las personas tienen en la red o en las aplicaciones. Las restricciones y permisos que deben tener para realizar sus tareas con los activos. El nivel de capacitación y formación educativa que necesitan tener acceso para manipularlos.
PROCESO			El flujo de actividades relacionadas a la atención a los clientes. el flujo necesario de información para la realización de transacción.	Análisis de los flujos de información de la organización y la manera en que la información transita de un área a otra, cómo son administrados los recursos en relación a la organización y manutención. En este ámbito, el activo de enfoque principal es del tipo usuario e información.	Identificar a las personas involucradas en el flujo de información, es posible evaluar la necesidad real de acceso que ellas tienen a los activos. Evaluar el impacto proveniente del uso indebido de la información por personas no calificadas.
FÍSICO		Los locales de trabajo de los equipos involucrados, las agencias o puestos de atención al cliente.	Los locales de almacenamiento de la información crítica. las centrales de proceso de información como los centros de proceso de datos, las salas de servidores, las centrales de procesamientos por teléfono, la sala caja fuerte.	Los locales de almacenamiento de la información crítica. las centrales de proceso de información como los centros de proceso de datos, las salas de servidores, las centrales de procesamientos por teléfono, la sala caja fuerte.	Identificar posibles fallas en la localización física de los activos tecnológicos. Evaluar el impacto de accesos indebidos a las áreas en donde se encuentran activos tecnológicos. Evaluar el impacto de desastres ambientales en la infraestructura de tecnología de la empresa.

Tabla 5. Riesgos y ámbitos.

La tabla 5 hace una descripción resumida de los ámbitos y riesgos que en de los cuales trata este capítulo. Además se define claramente cada uno de los aspectos más importantes que impactan las decisiones de las empresas en los diferentes ámbitos.

4.3 CUADRO COMPARATIVO Y CLASIFICACION DE LAS TECNICAS DE HACKING

	Técnica	Definición	Objetivo del ataque	Modo operacional	Consecuencias	Cómo detectarla ó prevenirla
ación	Scanning	Primera exploraciones para obtener información sobre la red de destino.	Indagar por el estado de los puertos de los host buscando vulnerabilidades.	Se intenta establecer conexión con varios puertos de la máquina objetivo.	Constantes avisos del firewall y utilización maliciosa de puertos abiertos.	Con buenas estándares de encriptación, con un firewall y realizando escáneres periódicos.
	Enumeración	Se recoge y se organiza toda la información alrededor a computadoras, redes, aplicaciones y servicios.	Obtener la mayor cantidad de información sensible que servirá para un ataque futuro.	Establecimiento de conexiones activas con el sistema y realización de consultas dirigidas.	Al conocer el sistema se pueden acceder a todos los recursos informáticos. Con esta técnica empiezan los ataques de Validación y Modificación.	Configurando los protocolos, configurando los servicios para que sólo muestren información necesaria y cambiando el password por defecto de todos los lugares.
	Sniffing	Permite escuchar la información cuando esta no va dirigida a la máquina que está capturando el tráfico.	Obtener información de todo el tráfico que pase por una red, no importa si los datos están encriptados.	Se usan analizadores de protocolos, que monitorizan y analizan el tráfico. Así se descifran los paquetes de datos.	Se ponen en evidencia elementos confidenciales tales como números de tarjetas e información sensible.	Enviando la información de manera encriptada, utilizando encriptación WPA y protegiendo routers con contraseñas.
n	Fuerza bruta	Técnica donde se intenta acceder por medio de la obtención de la clave.	Generar claves y probarlas en determinado servicio de autentificación ó archivo.	De todas las contraseñas encriptadas, se hallan todas las combinaciones posibles.	El intruso obtiene permisos sobre todo el sistema y puede infiltrarse fácilmente.	Bloqueando ó deshabilitando la cuenta al notarse intentos de inicio de sesión fallidos y cambiando contraseñas.
	Spoofing	Técnica donde se suplanta la identidad de un dispositivo en una red informática.	- Falsificar datos. - Adquirir información de una máquina. - Simular la identidad de otro.	En ARP Spoofing se introduce una dirección IP falsa a la asignación de direcciones MAC en la tabla ARP.	El riesgo más conocido es el de Phishing.	- Utilizando IP y tablas ARP estáticas. - Impidiendo que la dirección MAC sea modificada en los host.
	Hijacking	Técnica donde se intercepta y se roba una sesión de algún usuario para apropiarse de algún servicio.	Secuestrar una conexión ya establecida de manera legal por otro usuario con un servidor.	Por medio de un software sniffer se huelgan los paquetes que están circulando por la red y se envían paquetes al servidor.	- Acceso no autorizado a información. - Corte de la conexión entre el usuario legítimo y el servidor.	- Usando encriptación para codificar los datos. - Utilizando firewall, antivirus y antispyware. - Con protocolos de seguridad como https.
	Ingeniería Social	Método basado en engaño y persuasión, para obtener información significativa.	Obtener información y acceso a un sistema, con el fin de irrumpir en la seguridad de éste.	Puede operar con supuestos emails del banco a su cliente (Phishing) donde éste debe poner datos personales.	- Intromisiones a los sistemas y a las redes. - Vulnerabilidad en redes, servidores y cuentas de usuario. - Phishing.	No divulgando información sensible, implementando políticas de seguridad y adquiriendo un servicio técnico propio ó de confianza.
	Jamming	Bloqueo de un canal de comunicación con la intención de impedir el flujo de información.	Inundar con peticiones falsas, saturando los recursos de las máquinas destino, para bloquear los servicios normales.	Se satura al ordenador víctima con mensajes que requieren establecer conexión y dar respuestas.	- Saturación de los servidores. - Hacer una red inutilizable debido a la cantidad de tráfico.	Eliminando debilidades conocidas en los protocolo y la configuración del host y filtrando el tráfico.
	SYN Flooding	Consiste en mandar paquetes SYN y no contestar a los paquetes ACK producidos en la pila TCP/IP una espera de tiempo para recibir la respuesta del atacante.	Colapsar los recursos de las máquinas víctimas, accediendo el número de conexiones, para que no atiendan a usuarios legítimos.	Se falsean las direcciones IP de origen, haciendo múltiples intentos de conexión desde un mismo equipo.	- Saturación de los recursos de memoria. - Incapacidad de establecer conexiones adicionales. - Inundación de puertos, como Smtp y http.	- Blindando el servidor con un firewall del tipo stateful. - Diagnosticando de un sistema operativo actualizado. - Habilitando la protección SYN Cookie.
ión	Borrado de huellas	Modificación de los ficheros log del sistema operativo de la máquina asaltada, para borrar el rastro dejado por el atacante.	Ocultar todas las evidencias que puedan quedar al realizar cualquier intrusión pensando en ataques futuros.	Programando un zapper y borrando todos los logs que éste modifica tras su paso y sólo eliminando las entradas que correspondan a dichas sesiones.	- Posibilidad de ataque futuro, si no detectarse la intrusión a tiempo. - Pérdida de información de la mano del borrado de archivos.	Al detectar la intrusión se puede: - Cubrir los huecos de seguridad. - Evitar ataques posteriores. - Rastrear al atacante.

Tabla 6. Definición y comparación de técnicas de Hacking

La tabla 6 presenta información correspondiente a las técnicas de Hacking partiendo de los grupos en los cuáles se dividen estas técnicas que son: Monitorización, Validación, DOS (Denegación de Servicio) y Modificación. De cada una de las técnicas se expone una definición, su objetivo, el modo de operación, sus consecuencias y cómo detectarla ó prevenirla.

También se puede observar en la tabla que 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.

4.4 CONCLUSIONES

Este trabajo ha descrito la naturaleza y características de la importancia de la seguridad informática como es el tema de hacking empresarial, se ha visto que las organizaciones no concientizan y capacitan adecuadamente a los empleados, no se enseña por qué crear e implementar una cultura de seguridad informática empresarial y cuál es el impacto que esta traerá a la organización.Asimismo, se establecieron ciertos parámetros mínimos que ayudan a las personas interesadas, a discernir acerca de la creación e implementación de una cultura de seguridad informática empresarial tratadas en este documento de HACKING, en una situación empresarial.

La información recogida en este trabajo 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.

Las técnicas estudiadas se consideran las más importantes y hacen parte de una larga cadena de prácticas que pueden ser utilizadas de forma maliciosa para hacer daño, pero también se demuestra que contribuyen a corregir problemas de seguridad.

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.

4.5 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. Es aquí donde las políticas de seguridad informática deben implementarse para que todos los colaboradores de la organización entiendan su rol y cómo pueden participar para que la empresa crezca y siga siendo competitiva.

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.

4.6 REFERENCIAS BIBLIOGRAFICAS

- Amenazas: Tipos de ataques- http://www.buenastareas.com/ensayos/Amenazas-L%C3%B3gicas/2453279.html [Consulta: 29 agosto de 2011].

- DISA (Defense Information System Agency). http://www.disa.mil. [Consulta: 29 agosto de 2011]

- HOWARD, John D. Thesis. An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie MellonUniversity. 1995. EE.UU. http://www.cert.org. Capítulo 12–Página 168 .

- Acceso, Uso y Autenticación- http://www.buenastareas.com/ensayos/Amenazas-L%C3%B3gicas/2453279.html[Consulta: 30 agosto de 2011].

- Página de la Presidencia de la república de Colombia (hackeada)- http://wsp.presidencia.gov.co/Paginas/Presidencia.aspx[Consulta: 5 septiembre de 2011]

- Mi espacio(LEY 1273 DE 2010 DELITOS INFORMATICOS)- http://www.tareanet.edu.co/index.php?option=com_myblog&show=ley-1273-de-2010-delitos-informaticos-3768.html&Itemid=[Consulta: 1 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.

- Katos V, Furnell S. The security and privacy impact of criminalising the distribution of hacking Tools. Computer Fraud & Security. 2008. 2008 (7): 9-16.

- Promonegocios.net - http://www.promonegocios.net/mercadotecnia/empresa-definicion-concepto.html[Consulta: 12 de septiembre de 2011]

- Referencia Revista de Trejos

- 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]

- Concepto de análisis de riesgos - http://www.piramidedigital.com/Documentos/ICT/pdictsegurindadinformaticariesgos.pdf[Consulta: 14 de septiembre de 2011]

- Mundo en línea - http://www.mundoenlinea.cl/noticia.php?noticia_id=754&categoria_id=4 [Consulta: 15 de septiembre de 2011]

- Malagón C. Hacking Etico. Univeridad de Nebrija. 2009

- 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

- Nagaonkar S. Detecting stealthy scans and scanning patterns using threshold random walk. Canadá. 2008 - http://proquest.umi.com/pqdlink?did=1554499051&Fmt=7&clientId=79356&RQT=309&VName=PQD

- Gutiérrez R. Seguridad en VoIP: Ataques, Amenazas y Riesgos. Universidad de Valencia. 2008

- Moreno J. Seguridad Informática: Técnicas hacker. 2010 - http://informatica.gonzalonazareno.org

- Tori C. El Hacking Etico. Argentina, 2008. 328 pag.

- 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

- Barbhuiya F, Biswas S, Hubballi N, Nandi S. A host based DES approach for detecting ARP Spoofing. CICS 2011; 114-121

- Mieres J. Ataques informáticos - Debilidades de seguridad comúnmente explotadas. 2009

- 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

- Misra S, Dhurandher S, Rayankula A, Agrawal D. Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks. Comp. &Elect. Eng 2009; 36(2): 367-382

- 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.