

USERS

Esté preparado para combatir los nuevos ataques
que pueden afectar los datos de su empresa

Seguridad Informática por FABIAN PORTANTIER

Aprenda cómo
implementar
soluciones desde
la visión del experto

Red**USERS**.com



COLECCIÓN EXPERTOS EN TECNOLOGÍA

CONÉCTESE CON LOS MEJORES LIBROS DE COMPUTACIÓN

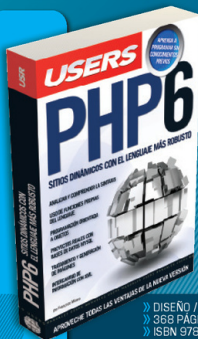
LLEGAMOS A TODO EL MUNDO
VÍA >OCA* Y **DHL****
 usershop.redusers.com
 usershop@redusers.com
 +54 (011) 4110-8700

* SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA. ** VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA



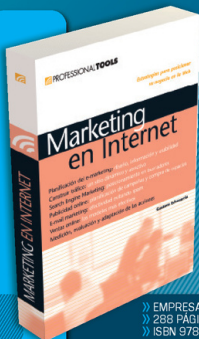
PREVENGA
Y SOLUCIONE
LOS DELITOS
INFORMÁTICOS
MÁS PELIGROSOS

» SEGURIDAD / EMPRESAS
» 352 PÁGINAS
» ISBN 978-987-663-008-5



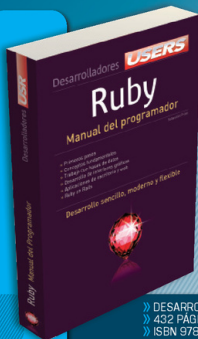
APRENDA A CREAR
SITIOS DINÁMICOS
CON EL LENGUAJE
MÁS ROBUSTO

» DISEÑO / DISEÑO WEB
» 368 PÁGINAS
» ISBN 978-987-663-039-9



ESTRATEGIAS
PARA POSICIONAR
Y CONSOLIDAR
SU NEGOCIO EN
LA WEB

» EMPRESAS / INTERNET
» 288 PÁGINAS
» ISBN 978-987-1347-82-7



DESARROLLO DE
ÚLTIMA GENERACIÓN
CON UN LENGUAJE
LIBRE Y FLEXIBLE

» DESARROLLO
» 432 PÁGINAS
» ISBN 978-987-1347-67-4

SEGURIDAD INFORMATICA

"SEGURIDAD INFORMÁTICA" POR **FABIAN PORTANTIER**

EL EXPERTO

FABIAN PORTANTIER

Especialista en implementación de
soluciones para la protección de datos





Título Seguridad Informática

Autor Fabian Portantier

Colección De Autor

Formato 17 x 24 cm

Páginas 192

Copyright © MMXII. Es una publicación de Fox Andina en coedición con DALAGA S.A. Hecho el depósito que marca la ley 11723. Todos los derechos reservados. Esta publicación no puede ser reproducida ni en todo ni en parte, por ningún medio actual o futuro sin el permiso previo y por escrito de Fox Andina S.A. Su infracción está penada por las leyes 11723 y 25446. La editorial no asume responsabilidad alguna por cualquier consecuencia derivada de la fabricación, funcionamiento y/o utilización de los servicios y productos que se describen y/o analizan. Todas las marcas mencionadas en este libro son propiedad exclusiva de sus respectivos dueños. Impreso en Argentina. Libro de edición argentina. Primera impresión realizada en Sevagraf, Costa Rica 5226, Grand Bourg, Malvinas Argentinas, Pcia. de Buenos Aires en I, MMXII.

ISBN 978-987-1857-29-6

Portantier, Fabian

Seguridad informática. - 1a ed. - Buenos Aires : Fox Andina;

Dalaga, 2012.

v. 1, 192 p. ; 24x17 cm. - (Seriada)

ISBN 978-987-1857-29-6

1. Informática. I. Título

CDD 005.3



ANTES DE COMPRAR

EN NUESTRO SITIO PUEDE OBTENER, DE FORMA GRATUITA, UN CAPÍTULO DE CADA UNO DE LOS LIBROS EN VERSIÓN PDF Y PREVIEW DIGITAL. ADEMÁS, PODRÁ ACCEDER AL SUMARIO COMPLETO, LIBRO DE UN VISTAZO, IMÁGENES AMPLIADAS DE TAPA Y CONTRATAPA Y MATERIAL ADICIONAL.

RedUSERS
COMUNIDAD DE TECNOLOGÍA



redusers.com

Nuestros libros incluyen guías visuales, explicaciones paso a paso, recuadros complementarios, ejercicios, glosarios, atajos de teclado y todos los elementos necesarios para asegurar un aprendizaje exitoso y estar conectado con el mundo de la tecnología.



LLEGAMOS A TODO EL MUNDO VÍA  **Y** 

* SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // ** VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

 usershop.redusers.com //  usershop@redusers.com

EL EXPERTO

FABIAN PORTANTIER

Fabián Portantier, nacido el 13 de octubre de 1985, en Buenos Aires, es propietario de Portantier Information Security, una consultora especializada en ayudar a las empresas con la implementación de soluciones para la protección de datos, haciendo uso intensivo de tecnologías de código abierto y productos personalizados, para satisfacer de forma completa las necesidades particulares de cada cliente. Durante varios años ha trabajado para una gran cantidad de empresas, en los sectores de telecomunicaciones, hotelería, educación, bancos y financieras, lo que le ha dado un sólido conocimiento sobre las amenazas y vulnerabilidades que pueden encontrarse en las diferentes infraestructuras tecnológicas, así como también el conocimiento de cuáles son las mejores maneras de protección para implementar en cada caso.

El interés por la tecnología se le despertó a una edad muy temprana, de modo que terminó el colegio secundario con el título de Técnico en Informática. Luego realizó varios cursos de capacitación en diferentes áreas, como diseño de redes (*Cisco Certified Design Associate*) y otros cursos de seguridad. Su conocimiento lo ha obtenido, fundamentalmente, de forma autodidacta, sobre la base de libros, apuntes y experiencia de campo adquirida en los diferentes trabajos realizados, como administrador de sistemas, programador, administrador de red y, más adelante, consultor en seguridad informática.

Su fanatismo por los sistemas GNU/Linux lo ha llevado a conocerlos profundamente y

a implementarlos en diversas oportunidades para brindar servicios de sitios web, bases de datos, correo electrónico, telefonía IP, monitoreo de redes, sistemas de prevención de intrusos y filtrado de conexiones. A través de sus años como administrador de servidores y redes, se ha vuelto un experto en la programación de scripts y herramientas en varios lenguajes, como Python, Ruby, PHP y Perl, con el objetivo de resolver diversas necesidades, como monitoreo de equipos, envío de alertas automáticas, copias de seguridad e interconexión entre varios sistemas.

Si bien ha tenido contacto con todas las distribuciones GNU/Linux más populares y con varios sistemas UNIX, su sistema operativo favorito es Debian GNU/Linux, el cual utiliza en sus estaciones de trabajo desde hace más de diez años, así como también en la mayoría de los servidores que instala. Ha realizado diversas auditorías de seguridad sobre diferentes infraestructuras, de forma tanto interna como externa, a través de metodologías de Penetration Testing y Análisis de Vulnerabilidades, generando reportes y asistiendo al personal en las tareas de toma de decisiones para solucionar los problemas de seguridad encontrados. Mantiene un particular interés por el alineamiento de las necesidades del negocio de las empresas con las necesidades y posibilidades que ofrece la tecnología, y fomenta la buena comunicación entre el personal técnico y los directivos. Esto lo ha llevado a enfocar sus trabajos en mejorar la seguridad de los sistemas teniendo en cuenta las

diferentes capacidades de inversión de las organizaciones, y aprovechando al máximo las soluciones que no requieren una gran



cantidad de recursos, lo que permite a las empresas aumentar enormemente sus niveles de seguridad, sin requerir la inversión de grandes sumas de dinero. Además de sus amplios conocimientos sobre el mundo del código abierto, ha trabajado con productos y tecnologías de diversas empresas, como Microsoft, Fortinet, Watchguard, Check-Point, Cisco, TrendMicro, Sophos, Symantec, VMWare, Oracle, D-Link, SMC, AlliedTelesis, Axis, HP, IBM, MicroTIK y Motorola. Con ellos ha implementado soluciones de autenticación centralizada, administración de usuarios y perfiles, filtrado de acceso a sitios web, optimización de redes, virtualización de infraestructuras, protección contra malware, seguridad en redes inalámbricas, videovigilancia y arquitecturas de servicios de alta disponibilidad.

Ha dictado varias capacitaciones, tanto a particulares como a empresas. Su metodología de enseñanza se enfoca en brindar a los alumnos fuertes bases teóricas, que luego se llevan a la práctica en laboratorios de pruebas; esto hace que las clases resulten entretenidas y permite que los asistentes entiendan exactamente qué están haciendo y por qué. Mantiene un gran interés por capacitar a las personas acerca de cuáles son las técnicas más utilizadas para atacar sistemas de información y cuáles son las formas más eficaces para protegerse de ellas. Una de sus últimas actividades ha sido la creación de una serie de cursos, formulados sobre la base de los objetivos de las certificaciones CISSP (**Certified Information**

Systems Security Professional) y CEH (**Certified Ethical Hacker**), con el propósito de capacitar tanto a profesionales que ya trabajan en el rubro, como a personas que quieran ingresar en el

mundo de la seguridad informática. Con un perfil orientado fuertemente a los ejercicios prácticos, incluso ha desarrollado herramientas de software que permiten explicar de modo didáctico todos los conceptos analizados en las partes teóricas de los cursos.

Ha desarrollado varias aplicaciones de código abierto, entre las que se encuentra DEWS, un proyecto creado íntegramente en el lenguaje de programación Python, que contiene varias herramientas destinadas a simplificar las tareas con las que debe lidiar un profesional de la seguridad informática. También la ha utilizado de forma intensiva en sus cursos, debido a que fue generada de forma tal que su uso sea sencillo, pero didáctico.

Escribe una serie de artículos denominado "Escuela de Hacking", acerca de las distintas herramientas y metodologías utilizadas en el mundo de la seguridad, tanto para proteger como para atacar sistemas informáticos. Con un alto contenido técnico, estos artículos permiten a los lectores aprender constantemente, realizando ejercicios paso a paso y descubriendo las diferentes técnicas de hacking

que pueden utilizarse para sacar el máximo provecho de las diversas tecnologías.

En su sitio web (www.portantier.com) pueden encontrarse varios recursos y un newsletter mensual gratuito, que trata sobre las últimas tendencias en seguridad y brinda trucos para que los profesionales puedan sacar el máximo provecho de las herramientas disponibles.

Dedicatoria:

A mi madre y a mi padre porque, en cierta forma, ellos también escribieron este libro.



PRÓLOGO

LA MIRADA DEL EXPERTO

POR FABIAN PORTANTIER

Desde que se me planteó la posibilidad de escribir un libro acerca de la seguridad informática, la idea del proyecto se volvió clara y concisa: "escribir un libro que describa las principales tareas de seguridad que las empresas deben llevar a cabo en sus sistemas, desde el punto de vista de un consultor especializado y teniendo en cuenta las limitaciones en los presupuestos para la seguridad".

Este objetivo no fue nada fácil de cumplir, debido a que la seguridad informática se encuentra asociada directamente con el término "costoso". Esta asociación, principalmente, es el resultado de pasar por alto los fundamentos y los principios básicos de la seguridad informática, con los cuales podemos idear medidas de protección sumamente efectivas, realizando inversiones muy pequeñas. En este libro expongo, sobre la base de mi experiencia, cuáles son las tareas que brindan mejores resultados con respecto a la seguridad, y que pueden ser implementadas sin realizar grandes inversiones de dinero.

He tenido la oportunidad de trabajar con muchas empresas, entre las que se encuentran bancos, financieras, hoteles y universidades, y he podido notar que, si bien cada infraestructura tecnológica es única, existen varios factores que son comunes para todas y cada una de ellas. Es en esos puntos comunes en los que tenemos que basarnos

para definir cuáles son los estándares por seguir, más allá de cualquier recomendación internacional (como ISO 27001), y poder plantearnos las bases de seguridad que vamos a utilizar. Después de eso, podremos implementar medidas que den respuesta a las particularidades puntuales de cada infraestructura. Ese es uno de los aspectos que vamos a aprender en este libro: a pensar inteligentemente y a aprovechar nuestros recursos de la mejor manera posible.

Luego de realizar varios Penetration Tests, análisis de vulnerabilidades, auditorías, consultorías y capacitaciones, he notado que la mayoría de las empresas están interesadas en aumentar la seguridad de sus sistemas, y ya se ha empezado a promover una conciencia en la cual los directivos reconocen la importancia de que sus sistemas se encuentren funcionando de forma correcta y segura. La idea de invertir en seguridad se ha establecido, por lo menos, en una gran parte de las organizaciones, y podemos afirmar que la puerta a las soluciones de seguridad está abierta pero, desgraciadamente, la mayoría de los proyectos se ven frenados a causa de los altos costos que representa encarar la mejora de la seguridad en una infraestructura tecnológica.

Es por eso que debemos considerar varios factores a la hora de plantear las posibles soluciones para implementar, y no centrarnos solamente en adquirir el último equipo que promete



aumentar la seguridad de toda la organización: también debemos tener en mente varios factores que van más allá de una tecnología puntual, y poseer una visión global, que nos permita analizar la situación de las empresas de manera total y nos dé la capacidad de reaccionar del mejor modo. Después de todo, la seguridad informática no es otra cosa que uno de los tantos procesos de negocio que debe llevar a cabo una empresa. Las organizaciones de Latinoamérica tienen que aprender a ajustar sus presupuestos e incluir a la seguridad informática dentro de sus políticas de inversión, mientras que los profesionales de la seguridad debemos acostumbrarnos a implementar medidas de control que sean adecuadas para nuestras capacidades económicas, basándonos en lo que dictan los estándares internacionales, pero sin dejar de considerar la situación local. Este libro llevará al lector por un recorrido que va desde los fundamentos principales de la seguridad informática, aquellos que se utilizan para escribir los documentos más reconocidos así como también para desarrollar los sistemas de más alto nivel; hasta trucos específicos para los sistemas más utilizados en las infraestructuras tecnológicas de la actualidad, aquellas cosas que solamente los profesionales con experiencia en la práctica pueden conocer y que comparto con los lectores para que puedan desenvolverse de forma rápida en el mundo de la seguridad, contando con una base sólida que les permitirá llevar a cabo sus tareas de la mejor manera posible. Escrito pensando en la situación actual de las empresas, y analizando las alternativas que tenemos para brindar soluciones que presenten una excelente eficacia con el uso de bajos recursos, esta obra le será de utilidad tanto al estudiante que busca conocer la visión de un experto, para formar su carrera,

así como también a la persona que ya se desempeña como profesional de la seguridad, y que busca perfeccionar sus conocimientos y mejorar sus aptitudes laborales. Con muchas referencias a excelentes productos y fuentes de información, el lector podrá descubrir una gran cantidad de herramientas para construir su 'arsenal de trabajo' y tener la capacidad de dar respuesta a varias situaciones diferentes. La seguridad informática es, sin dudas, una de las áreas de estudio más apasionantes en la actualidad. Tanto es así, que mi profesión, muchas veces, es vista más como un juego que como un trabajo, debido a requiere un proceso de aprendizaje constante, que, además de mejorar nuestras capacidades para asegurar sistemas, entender cómo funcionan las tecnologías y programar aplicaciones, nos divertimos muchísimo. Pero más allá de eso, hay que reconocer que estamos hablando de una profesión que requiere mucho de nosotros debido, justamente, a este proceso de aprendizaje constante, que nos obliga a leer permanentemente acerca de los nuevos productos y tecnologías que se están implementando en el mercado, estar al tanto de cuáles son las metodologías más efectivas y tener en mente qué es lo que nos depara el siguiente paso del mundo de la informática, con el objetivo de estar preparados

para combatir los nuevos ataques a los cuales tendremos que enfrentarnos.

Felicitó al lector por tener la iniciativa de leer este libro, y lo aliento para que lo haga de manera entusiasta, pero detenida, prestando atención a cada uno de los capítulos que se desarrollarán a partir de las siguientes páginas. La lectura es una de las actividades más fascinantes que

podemos llevar a cabo. Espero con ansias que podamos compartir este viaje por el mundo de la seguridad informática y todas las particularidades que encierra.

Saludos cordiales



CÓMO LEER ESTE LIBRO DE UN VISTAZO

Como podremos observar, éste libro no pretende explicar en detalle cada una de las tecnologías utilizadas, porque se necesitarían decenas de miles de hojas para hacerlo. En cambio, podemos afirmar que vamos a exponer algunos de los trucos y consejos más efectivos que un profesional puede conocer. Éste libro se encuentra dividido en dos partes de tres capítulos cada una. La primera, explica los fundamentos de la seguridad y los procesos que debe tener en cuenta toda organización que quiera mantener la seguridad de sus datos. La segunda, más técnica, profundiza en las herramientas y técnicas más utilizadas para asegurar sistemas operativos, dispositivos de telecomunicaciones y las nuevas tecnologías emergentes.

Folio. páginas
y Nombre del
Capítulo

Recomendados. en estos
apartados encontrarán links a
sitios, aplicaciones y artículos que
les resultarán de gran ayuda.

Frases destacadas.
resaltan una idea por
encima del resto del texto.
No están aisladas, sino que
forman parte del cuerpo,
por lo que se deben leer
como parte del mismo.

2. GESTIÓN DE LA INFORMACIÓN

Una vez que hayamos completado la tabla de amenazas, procederemos a investigar qué vulnerabilidades tenemos en nuestros sistemas. Ya sea a través del análisis minucioso de las configuraciones, el uso de herramientas automatizadas o cualquier otro método, obtendremos una lista de cada uno de los activos, con las vulnerabilidades que presenta. Es necesario emplear varios métodos para recabar este tipo de información, como analizar configuraciones, leer manuales y utilizar herramientas automatizadas, pero debemos saber que es necesario unificar estos datos, para trabajarlos de manera adecuada. Para poder hacer uso de toda la información recopilada, debemos ordenarla con el fin de poder realizar comparaciones y filtrados. Esto puede lograrse a través de herramientas especializadas, la creación de alguna pequeña

Figura 13.1. En la imagen vemos un vistazo de vulnerabilidades conocidas por activo, y las amenazas que podrían aprovecharlas para causar daños.

Activo	Vulnerabilidad	Amenaza probable
Estaciones de trabajo	- Fallas de antivirus. - puertos USB sin restricciones. - Usuario Guest habilitado.	- Malware. - Usuarios desconocidos. - Hackers.
Servidores	- Firewall deshabilitado. - Sistema Operativo desactualizado. - Sin copias de respaldo de los datos.	- Hackers. - Malware. - Usuarios desconocidos. - Falla de hardware.
Router externo	- Telnet habilitado. - Falta de redundancia de hardware. - ACL no definidos.	- Hackers. - Falla de hardware. - Hackers.

Tablas. una forma
rápida y efectiva para
hacer comparativos.

RECOMENDADOS

Algunas de las herramientas gratuitas que podemos utilizar para automatizar la búsqueda de vulnerabilidades son **OpenVAS** (www.openvas.org), **Nessus Community Edition** de los mismos creadores de **Metasploit Framework** (www.rapid7.com) y **Microsoft Baseline Security Analyzer**, que sirve solo para sistemas **Microsoft** (www.microsoft.com).

herramienta con una base de datos relacional o haciendo un uso exhaustivo de plantillas de cálculo. Lo importante de contar con una tabla de activos con vulnerabilidades explotables es que nos garantiza la capacidad de asignar prioridad a aquellos que conen más peligro. Utilizaremos esta tabla en el siguiente paso.

Como final del proceso de identificación, obtendremos una tabla con los niveles de riesgo que tiene cada activo sobre la base de cada una de las vulnerabilidades que posee. Con estos podremos

una organización, en que se alcance los niveles implementando el adecuado, para evitar la información y fraudes, a menos profesionales para la organización y en todos los niveles.

NUESTRO PAN

nos obligó esta carrera, en por los avances tecnológicos.

Tener la capacidad de asegurar un sistema implica tener el entendimiento de cómo este funciona

Por lo tanto, es posible estar ampliamente capacitados en varias tecnologías, y mantener un estudio constante acerca de los cambios y las nuevas posibilidades que se abren año tras año. En varias carreras, para tener éxito necesitamos alcanzar algo que se llama **superespecialización**. Esto quiere decir que tendremos un conocimiento extremadamente avanzado acerca de temas específicos. Por ejemplo, hay profesionales que están superespecializados en **tecnologías de storage**. Esto les permite ser en primer nivel, con la capacidad de solucionar prácticamente cualquier tipo de problema que pueda surgir dentro de su área de estudio.

En el caso de la seguridad informática, la superespecialización no sirve. Estamos hablando de una carrera en la cual necesitamos trabajar con todas las tecnologías que utiliza una organización, las redes, los sistemas operativos, el storage, las aplicaciones, etcétera. Pero, obviamente, no podemos ser expertos en todo, sino que será preferible tener un entendimiento amplio de cada una de estas tecnologías. Esto nos dará una visión generalizada de toda la infraestructura tecnológica, con lo cual tendremos la capacidad de implementar soluciones de seguridad para

Microsoft, uno de los más largos de haber pasado varios años en prisión, se decidió a brindar servicios como profesor de la seguridad y a escribir libros sobre el tema.

LA SEGURIDAD EN LAS EMPRESAS

Las empresas, de forma consciente o inconsciente, han involucrado sus procesos de negocio mediante a los sistemas de información. Siempre con el fin de volverse más productiva, ahorrar costes y poder realizar negocios en todas partes del mundo, cada una de las operaciones de una empresa se ha transformado en parte de una aplicación informática.

La información que años atrás era almacenada en papel o en fichas se guarda en un lugar conocido, íntegro, copiable y distributable a voluntad, ahora se encuentra dispersa en forma de correos, vídeos, dentro de varios medios de almacenamiento, como memorias USB, discos duros, dispositivos ópticos, y otros. Esto ha creado una amplia diversidad de fuentes de información, que nosotros estamos encargados de proteger.

Dentro de las filas de una organización que se rige por un presupuesto, nuestros recursos para brindar protección y seguridad están limitados. Algunas empresas asignan más capital a la seguridad informática que otras, pero lo cierto es que todos, en mayor o menor medida, nos encontramos limitados en cuanto a los recursos de que podemos disponer para realizar nuestros fines.

Consejos útiles.

estas frases son tips ideales para repasar en el día a día.

Como buenos profesionales de la seguridad, debemos tener en cuenta las necesidades de la organización, con el fin de alinear las prácticas de seguridad con los objetivos de la empresa

Esto es imprescindible si pretendemos integrar la seguridad como uno de los procesos de negocio



Figura 13. Límite y otros medios sociales se presentan entre un desafío para la seguridad, debido a que pueden ser utilizados para divulgar, por ejemplo, también, para divulgar información confidencial

LA SEGURIDAD COMO PROCESO DE NEGOCIO

Continuando, adelantándose a los acontecimientos...



Figura 15. El servicio gratuito *InfoSec* es proveído por *Hispano-Sistemas* (www.hispano.com) y ofrece un canal RSS con una notificación de seguridad diaria. Éste es una excelente forma de mantenerse actualizado.

toda la información, teniendo en cuenta todos los aspectos que la afectan.

TÍTULOS Y CERTIFICACIONES

La industria tecnológica tiene la particularidad de que no es necesario contar con títulos o certificaciones que avalen nuestros conocimientos para que podamos ser profesionales. Si bien este tipo de reconocimientos puede darnos las puertas a diferentes oportunidades laborales, no son totalmente necesarios. Tomando otros caminos como, por ejemplo, ya sea la medicina, la abogacía o la contaduría, todas requieren, obligatoriamente, el título de grado para poder ejercer. Dicho esto, muchas veces surge el interrogante de si es necesario o no poseer certificaciones que acrediten nuestros conocimientos profesionales. Aquí como en muchas otras cuestiones, la respuesta es "depende". Siempre debemos tener en cuenta el costo y el beneficio asociado a tener una acreditación. El costo puede ser económico, el tiempo de estudio que nos demande, etcétera. También debemos considerar el cargo

profesional al que aspiramos, debido a que, en ciertas organizaciones, es imprescindible tener un título para obtener trabajos. Por supuesto, la seguridad informática se habla más de certificaciones que de títulos de grado, por ser estas más flexibles y estar más actualizadas. En caso de que queramos diferenciarnos del resto, y de acuerdo con el perfil profesional que busquemos, podemos optar por diferentes certificaciones. Algunas de ellas son **CCSP**, **Security+ CSA**, **CISSP**, **CEM**, entre otras.

EN LA PRÁCTICA PROFESIONAL

Capacitarnos constantemente mediante nuevos cursos, ágiles y receptivos a nuevos conocimientos y experiencias. A medida que pasa el tiempo, vemos a notar que nos es cada vez más difícil la actualización técnica y entender cómo funcionan los sistemas. Incluso parece a tener la capacidad de estudiar cosas que nosotros no explicamos, debido a la experiencia que vemos desarrollando y a que el diseño de los sistemas y las herramientas suele seguir ciertos patrones comunes, que se repiten en la mayoría de las soluciones. También es muy recomendable que constantemente probemos nuevas prácticas y tecnologías, aunque no vayamos a utilizarlas. Para como en cualquier caso las herramientas que tenemos a nuestra disposición y cuáles son las nuevas capacidades que se nos ofrecen. Esto nos permite analizar cuáles son las mejores prácticas o implementar esas funcionalidades nosotros mismos. Dicho al final de las últimas tendencias del mercado es un requisito indispensable para mantenernos como profesionales de este



© REUTERS.COM

Estadísticas, en

materia de seguridad es fundamental conocer la situación del entorno. Estos números brindan un panorama rápido y eficaz.

Si seguimos nuestra línea de servicio, estamos ahorrando el dinero que perdíamos al no poder trabajar. Si los demostremos a nuestros clientes, un compromiso con la seguridad de sus datos y contribuir a un servicio de primer nivel, estaremos ganando más dinero porque atraeremos más clientes y mantendremos contentos a los que ya tenemos. Esto son, simplemente, dos ejemplos de cómo podemos utilizar la seguridad informática con objetivos directamente relacionados con el negocio.

Las empresas ven como obstáculos de seguridad la falta de apoyo de la gerencia (15,21%) y la falta de entendimiento (18,47%)

Fuente: *Informe Latinoamericano de Seguridad de la Información A33* (2010)

Para todo profesional de la seguridad, es de suma importancia tener la capacidad de exponer estos conceptos ante los directivos de una empresa con el objetivo de que se les otorgue su atención. Como cada persona habla su propio lenguaje, dependiendo de su área de especialización, es imposible que podamos convencer al gerente de marketing sobre los beneficios del nuevo sistema de protección de datos personales, si le marcamos que lo bueno del sistema es que está programado en Python y que cada una de las capacidades de abstracción que permite extender el sistema por medio de plugins, que se desarrollan utilizando la API del fabricante. Seguramente, la palabra "Python", dejará de prestarnos atención. Una situación muy distinta puede darse si le explicamos que tener un sistema de protección de datos personales permite asegurar a nuestros



Figura 14. Preguntas en cuenta con quién estamos hablando y entendiendo correctamente es que al ser y cómo hacerlo. De lo contrario, es muy probable que no nos presten la atención que deseamos.

clientes que sus datos se encuentran protegidos por una tecnología muy avanzada, que garantiza que nuestra organización cubra de ellos y de sus intereses. Siempre debemos hablar en el "lenguaje" de nuestro interlocutor, está es una de nuestras tareas como vendedores profesionales.

MUST KNOW

Debemos recordar que, cuando hablamos de recursos, no tenemos que considerar solamente el dinero, también debemos tener en cuenta los recursos humanos y los tiempos de los que disponemos, las cuales, muchas veces, limitan siendo factores tanto o más importantes que los recursos monetarios.

EN LA PRÁCTICA PROFESIONAL

Es una excelente idea que, antes de hablar con personas ajenas al ámbito de la seguridad informática, tengamos unos minutos para reflexionar acerca de qué ventajas debemos exponer. Podemos en la piel de la otra persona y analizar sus necesidades, lo que nos permitirá conectar mejor con cada uno de los integrantes de la empresa.

Must know. estos recuadros contienen información que no podemos desconocer para entender por completo el objetivo del capítulo.

En la práctica profesional. para reforzar los aspectos teóricos del libro, destacamos en este recuadro los puntos claves del libro llevados a la realidad.

CONTENIDOS

SEGURIDAD INFORMÁTICA

SOBRE EL AUTOR	4
PRÓLOGO	6
EL LIBRO DE UN VISTAZO	8

CAPÍTULO 1

LA SEGURIDAD INFORMÁTICA

INTRODUCCIÓN	14
LA SEGURIDAD COMO PROFESIÓN	16
EL ESTUDIO, NUESTRO PAN DE CADA DÍA	18
Títulos y certificaciones	19
METODOLOGÍAS DE TRABAJO	20
Defensa en profundidad	21
EL PRINCIPIO KISS	22
DESDE ARRIBA HACIA ABAJO	24
LA SEGURIDAD EN LAS EMPRESAS	26
LA SEGURIDAD COMO PROCESO DE NEGOCIO	26
MÉTRICAS DE SEGURIDAD	28
MEJORA CONTINUA	28

CAPÍTULO 2

GESTIÓN DE LA SEGURIDAD

INTRODUCCIÓN	32
EL AUTOCONOCIMIENTO	34
ANÁLISIS CUALITATIVO VS. CUANTITATIVO	37
AMENAZAS Y VULNERABILIDADES	38
IMPLEMENTACIÓN DE CONTROLES	44
POLÍTICAS Y OTROS DOCUMENTOS	46

Estándares	48
Procedimientos	49
RESPONSABILIDADES	49
El equipo de seguridad	50
Capacitación al personal	52
Dueños, custodios y usuarios de datos	53

CAPÍTULO 3

CONTINUIDAD DEL NEGOCIO

INTRODUCCIÓN	56
COPIAS DE RESPALDO	57
MONITOREO	60
CONTROL DE CAMBIOS	63
AMBIENTES DE PRUEBAS Y PRODUCCIÓN	65
GESTIÓN DE INCIDENTES	66
BIA, BCP Y DRP	70
SITIOS DE CONTINGENCIA	74
Sitio de contingencia en frío (Cold Site)	74
Sitio de contingencia tibio (Warm Site)	74
Sitio de contingencia en caliente (Hot Site)	74

CAPÍTULO 4

TELECOMUNICACIONES

INTRODUCCIÓN	76
INVENTARIO DE DISPOSITIVOS	77
SWITCHES INTELIGENTES	77
ARPALERT	77

SCRIPTING	77
ROUTERS Y SWITCHES	78
PORT SECURITY	80
DHCP SNOOPING	82
CUENTAS DE ACCESO CENTRALIZADAS	83
Tacacs+	83
Radius	83
Diameter	83
UTILIZACIÓN DE SERVIDORES SYSLOG	84
FIREWALLS	84
REDES INALÁMBRICAS	86
PREVENCIÓN DE INTRUSOS	90
IMPLEMENTACIÓN DE SISTEMAS IDS	92
ADMINISTRACIÓN REMOTA	93
CLI VS. TUI VS.GUI VS. WUI	94
PROTOCOLOS TCP/IP	95
SSH	96
TLS	97
SMTP, IMAP Y POP3	97
HTTP Y FTP	98
DHCP	99
DNS	100
SNMP	101
DISEÑO DE REDES SEGURAS	102
ZONAS DESMILITARIZADAS	104
Firewalls	104
Router	105
Servidor	105
SEPARACIÓN DE VLANS	106
REDES PRIVADAS VIRTUALES	108

CAPÍTULO 5

SISTEMAS OPERATIVOS

INTRODUCCIÓN	110
WINDOWS VS. UNIX	111
CONSEJOS PARA SISTEMAS WINDOWS	112
CONSEJOS PARA SISTEMAS UNIX	113
HARDENING	114
NETWORK ACCESO CONTROL	118
Tecnología Nac	118
MALWARE	119
PROTECCIÓN DE CAPAS	121
FIREWALLS	122
BACKUPS	124
HERRAMIENTAS SIN AGENTES	124
HERRAMIENTAS EN AGENTES	124
SCRIPTS PERSONALIZADOS	124
RECUPERACIÓN COMPLETA	125
AUTENTICACIÓN MULTIFACTOR	125
TOKENS O SMART CARDS	125
TOKENS VIRTUALES	126
TARJETAS DE COORDENADAS	126
BIOMETRÍA	127
SERVIDORES DE AUTENTICACIÓN	128
ANÁLISIS DE LOGS	130
SERVIDORES CENTRALIZADOS	131
ADMINISTRACIÓN REMOTA	132
PORT KNOCKING	133
WMI	133
RDP Y VNC	136
SSH	136
SNMP	137
WEBMIN	137

DETECCIÓN DE INTRUSOS	137
HONEYPOTS	139
GESTIÓN DE PARCHES	141

CAPÍTULO 6

NUEVAS TENDENCIAS

INTRODUCCIÓN	144
WEB 2.0	115
REDES SOCIALES	115
GOOGLE HACKING	146
PHISHING Y ROBO DE IDENTIDAD	147
SERVICIOS DE MENSAJERÍA	149
MENSAJERÍA INSTANTÁNEA	150
TRANSFERENCIAS DE ARCHIVOS	151
FUGA DE INFORMACIÓN	152
COMUNICACIONES NO DESEADAS (SPAM)	153
VOIP	154
ESPIONAJE DE COMUNICACIONES	155
VIDEOCONFERENCIAS	155
VIRTUALIZACIÓN	156
Asegurar los equipos de Host	156
Asegurar los medios de almacenamiento	157
Asegurar las máquinas virtuales	157
Utilizar las plantillas de máquinas virtuales	157
La gestión de la infraestructura virtual	157
Filtros físicos en las zonas de alta criticidad	157
Los sistemas host son tan críticos como la máquina virtual que corre sobre ellos	158
Separar una red para administración	158
Garantizar la conectividad de la infraestructura con las demás redes	158
Implementar separación de tareas para la gestión de la infraestructura	159

Contar con redundancia de equipos	159
CLOUD COMPUTING	159
Utilizar encriptación de discos	160
Asegurar copias de respaldo de los datos	160
Contratar solo a proveedores de confianza	160
La privacidad de los datos	161
DIFERENCIAS CON OTROS SERVICIOS	161
TECNOLOGÍA MÓVIL	162
DISPOSITIVOS PORTÁTILES	162
TELETRABAJO	163
ATAQUES DIRIGIDOS	164
Denegación de servicios (DOS)	164
El peligro de la perseverancia	166
IPV6	166
EXPECTATIVAS PARA EL FUTURO	167

APÉNDICE

ETHICAL HACKING

CLASIFICACIONES	173
INTERNO/EXTERNO	174
CAJA BLANCA/CAJA NEGRA	174
RECONOCIMIENTO	175
ESCANEO	175
Tipos de escaneo	176
Identificación de servicios	177
Explois	178
Informe Técnico	180
¿QUE SIGUE?	181

SERVICIOS

AL LECTOR

ÍNDICE TEMÁTICO	184
CATÁLOGO	188

CAPÍTULO 1

LA SEGURIDAD INFORMÁTICA

PARA APROVECHAR ESTE CAPÍTULO

» **DESTACARLO** COMO MATERIAL DE CONSULTA PERMANENTE, YA QUE MUCHAS DE LAS BASES QUE AQUÍ SE EXPLICAN VAN A UTILIZARSE DURANTE EL RESTO DEL LIBRO.

» **RECORDAR** QUE NO PODEMOS CENTRARNOS ÚNICAMENTE EN LOS ASPECTOS TÉCNICOS, SINO QUE TAMBIÉN DEBEMOS CONSIDERAR LOS ASPECTOS ADMINISTRATIVOS DE LA PROFESIÓN.

» **ANALIZAR** CADA CONCEPTO EXPUESTO EN ESTE CAPÍTULO Y COMPARARLO CON NUESTRA FORMA ACTUAL DE TRABAJO. VER EN QUÉ PODEMOS MEJORAR.

LA SEGURIDAD INFORMÁTICA

En este capítulo aprenderemos a:

Objetivo 1 Obtener una visión global de la seguridad informática.

Objetivo 2 Diferenciarnos como verdaderos profesionales.

Objetivo 3 Comprender los objetivos de la seguridad en las empresas.

Objetivo 4 Entender las metodologías que atraerán el éxito a nuestro trabajo.

Con el correr de los años, los seres humanos dependemos cada vez más de la tecnología para mantener nuestro estilo de vida. Ya sea para que las empresas puedan desarrollar sus negocios o para que las personas realicen sus tareas cotidianas, la tecnología siempre está ahí, simplificando las cosas. Esto ha llevado a una dependencia en la cual no todas son ventajas. Si nos situamos unos veinte años atrás, podemos imaginar que la pérdida de conectividad con Internet o el mal funcionamiento de un sistema resultaba algo bastante molesto. Hoy en día, la pérdida de conectividad significa que una empresa quede prácticamente inoperante.

Figura 1. El robo de identidad es una de las actividades delictivas que han crecido con el uso de la tecnología. En respuesta a esto, se han creado varios sitios que ofrecen ayuda e información para combatir este tipo de crímenes, como es el caso de www.ftc.gov/bcp/edu/microsites/idtheft

The screenshot shows the FTC website titled "DEFIENDASE CONTRA EL ROBO DE IDENTIDAD" (Defend Yourself Against Identity Theft). The page is in Spanish and includes a navigation bar with links like "Consumidores" and "English". The main content is organized into three columns: "DETENER" (Prevent), "DETECTAR" (Detect), and "DEFENDERSE" (Defend). Each column provides specific advice on how to protect oneself from identity theft. A sidebar on the right features a video player and links to important topics and reports.

DEFIENDASE CONTRA EL ROBO DE IDENTIDAD
COMISIÓN FEDERAL DE COMERCIO

CONSUMIDORES | ENGLISH

DETENER DETECTAR DEFENDERSE

Cada año, millones de personas son víctimas del robo de identidad. La Comisión Federal de Comercio (Federal Trade Commission, FTC), la agencia nacional de protección de los consumidores, quiere que usted tenga la información necesaria para defenderse contra el robo de identidad. Si bien no existe una manera infalible de evitar el robo de identidad, es importante que usted sepa cómo.

DETENER a los ladrones de identidad protegiendo su información.

DETECTAR actividad sospechosa monitoreando regularmente sus cuentas financieras.

DEFENDERSE contra el robo de identidad en cuanto lo sospeche.

Estos enlaces incluyen toda la información que necesitará para educar a su comunidad a **detener, detectar y defenderse** contra el robo de identidad. Todos estos materiales están disponibles en el Kit de Educación para Consumidores sobre el Robo de Identidad en español y en inglés.

Temas importantes

Utilice nuestros materiales en su comunidad

Ver el video

Consejo de Trabajo del Presidente sobre Robo de Identidad (en inglés)

Informe de la FTC sobre la

A medida que las personas volcamos nuestras vidas hacia la tecnología, almacenamos información personal, registros médicos y balances de cuenta en sistemas informáticos. Y a medida que las organizaciones confían en la tecnología para hacer negocios, establecer comunicaciones y transferir fondos, empiezan a aparecer otras personas, no tan bien intencionadas, que ven la tecnología como una excelente plataforma para cometer acciones ilícitas, con el fin de obtener beneficios a costa de los demás. Debido a esto, los daños por robo o pérdida de información crecen a la par de nuestra dependencia tecnológica. Muchos criminales optan por utilizar la tecnología como herramienta, ya sea para cometer nuevas formas de crimen o para complementar que ya están difundidas. En el caso de las empresas, debemos sumar los intereses que puede llegar a tener la competencia por obtener datos confidenciales, como planes de marketing, balances financieros, datos de clientes, etcétera.

“Además de malware y virus, nos referimos a programas especializados en robar información bancaria, en extraer datos personales y en realizar acciones direccionadas al enriquecimiento ilícito

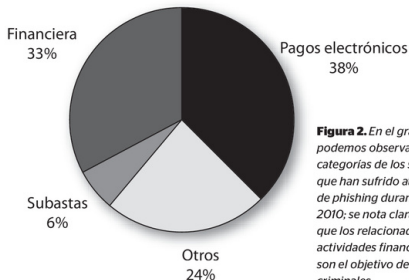


Figura 2. En el gráfico podemos observar las categorías de los sitios que han sufrido ataques de phishing durante 2010; se nota claramente que los relacionados con actividades financieras son el objetivo de los criminales.



Es por eso que se ha vuelto necesario establecer mejores prácticas y crear herramientas destinadas a proteger la información de las personas y las organizaciones. Todos estos esfuerzos se conocen como **seguridad informática**, y han ido evolucionando hasta convertirse en un área de estudio que dio lugar a la existencia de profesionales dedicados, exclusivamente, a proteger la información.

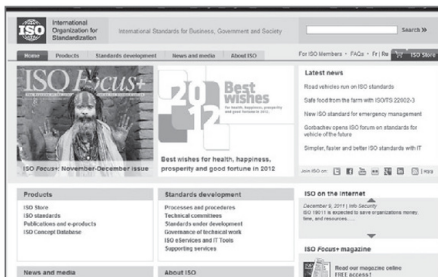
LA SEGURIDAD COMO PROFESIÓN

Ser un profesional de la seguridad informática es una tarea bastante particular, debido a que, como veremos más adelante, nos llevará a tener relación con todas las áreas de una empresa. Es imperativo que tengamos un conocimiento amplio acerca de cómo funciona la organización para la que estamos trabajando, sus procesos de negocio, sus objetivos y otros aspectos. Solo de esta manera podremos tener una visión global acerca de cómo es adecuado proteger la información con la que trabajamos. Esta es una profesión para la cual precisamos estudiar una gran cantidad de material, teniendo en mente varios estándares y metodologías, lo que puede llevarnos a pensar solamente en

“**Debemos ser objetivos con las medidas de seguridad, considerando los intereses de la organización como principal motor de acción**

lo que debería hacerse y olvidarnos de lo que puede hacerse. Lo que **debería hacerse** es exactamente lo que dice la norma **ISO 27000**. Si nos detenemos a pensar, esta es una norma escrita por profesionales destacados, con una amplia experiencia y un entendimiento claro de lo que es la seguridad de la información.

Figura 3. ISO (www.iso.org) es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación. Su función principal es buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.



Entre 2008 y 2009, los ataques informáticos para realizar fraudes financieros mostraron un crecimiento del 66%

(Fuente: CSI Survey 2009)

Lo que **puede hacerse** son las mejores prácticas que podemos implementar, muchas veces, basándonos en normas como la ISO 27000, pero considerando que nuestros recursos son limitados. Incluso en las organizaciones más grandes, los recursos tienen un límite; la única diferencia es la cantidad de ceros a la derecha que tienen esos límites.

Aquí entra en juego nuestra capacidad para poner los pies sobre la tierra y discernir entre lo que dice una norma de mejores prácticas acerca de todo lo que debería hacerse para proteger la información de una organización, y los recursos con los que cuenta una entidad para implementar medidas de seguridad, sin entrar en quiebra por tener que realizar dichas inversiones.

Tengamos en cuenta que los objetivos de las organizaciones son variados: captar más clientes, ganar más dinero, brindar mejores servicios, tener los costos más bajos, y otros, pero

no existe ninguna organización en la que el objetivo principal sea “tener las mejores medidas de seguridad informática”

DEL EXPERTO

En la práctica profesional

En lo que a medidas de seguridad informática se refiere, no es tan importante la cantidad de recursos que invertimos, sino que más bien debemos considerar la inteligencia con la cual implementamos dichas medidas. Actualmente existen muchas soluciones gratuitas o de bajo costo, que podemos implementar para simplificar nuestras tareas. Debemos considerar que la implementación de medidas de seguridad va a representar no solamente una inversión económica, sino también una inversión de tiempo. Existen varias herramientas de seguridad que pueden permitirnos reducir los tiempos que nos lleva realizar ciertas tareas, por lo que debemos considerar las capacidades técnicas de estas herramientas, si no también los beneficios que pueden traernos en nuestro día de trabajo. Debido a que estas

herramientas simplifican las tareas diarias, podemos no solamente aumentar la seguridad de nuestros sistemas, y además ahorrar recursos, tanto de tiempo como de dinero. Este es uno de los factores que marcan la diferencia entre un novato y un verdadero profesional. que senectus et netus et malesuada



como todo individuo en una organización, nuestro trabajo es ayudar que esta alcance sus objetivos. Nosotros lo haremos implementando las medidas de seguridad adecuadas, para evitar pérdida de datos, robo de información y fraudes. Teniendo esto en cuenta, seremos profesionales que aporten verdadero valor a la organización y estaremos muy bien vistos en todos los niveles jerárquicos de la empresa.

EL ESTUDIO, NUESTRO PAN DE CADA DÍA

Está implícito que, si hemos elegido esta carrera, tenemos una gran afición por los avances tecnológicos y el estudio de los sistemas.

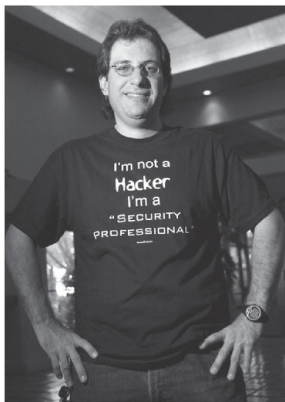


Figura 4. En la foto, Kevin Mitnick, uno de los hackers más famosos, quien luego de haber pasado varios años en prisión, se dedicó a brindar servicios como profesional de la seguridad y a escribir libros sobre el tema.

“Tener la capacidad de asegurar un sistema implica tener el entendimiento de cómo este funciona

Por lo tanto, es preciso estar ampliamente capacitados en varias tecnologías, y mantener un estudio constante acerca de los cambios y las nuevas posibilidades que se abren año tras año. En varias carreras, para tener éxito necesitamos alcanzar algo que se llama superespecialización. Esto quiere decir que tendremos un conocimiento extremadamente avanzado acerca de un tema específico. Por ejemplo, hay profesionales que están superespecializados en **tecnologías de storage**. Esto les permite ser de primer nivel, con la capacidad de solucionar prácticamente cualquier tipo de problemas que pueda surgir dentro de su área de estudio.

En el caso de la seguridad informática, la superespecialización no sirve. Estamos hablando de una carrera en la cual necesitamos trabajar con todas las tecnologías que utiliza una organización: las redes, los sistemas operativos, el storage, las aplicaciones, etcétera. Pero, obviamente, no podemos ser expertos en todo, sino que será preferible tener un entendimiento amplio de cada una de estas tecnologías. Esto nos dará una visión abarcativa de toda la infraestructura tecnológica, con lo cual tendremos la capacidad de implementar soluciones de seguridad para

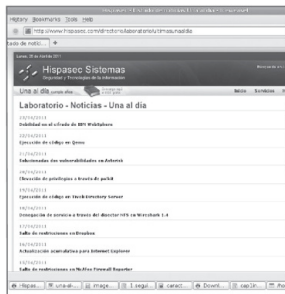


Figura 5. El servicio gratuito *Una al día*, provisto por Hispasec Sistemas (www.hispasec.com), brinda un canal RSS con una noticia de seguridad diaria. Esta es una excelente forma de mantenernos actualizados.

toda la organización, teniendo en cuenta todos los aspectos que la afectan.

TÍTULOS Y CERTIFICACIONES

La industria tecnológica tiene la particularidad de que no es necesario contar con títulos o certificaciones que avalen nuestros conocimientos para que podamos ser profesionales. Si bien este tipo de reconocimientos puede abrirnos las puertas a diferentes oportunidades laborales, no son totalmente necesarios. Tomando otras carreras como ejemplo, ya sea la medicina, la abogacía o la contaduría, todas requieren, obligatoriamente, el título de grado para poder ejercer. Dicho esto, muchas veces surge el interrogante de si es necesario o no poseer certificaciones que acrediten nuestras competencias profesionales. Aquí, como en muchas otras cuestiones, la respuesta es: “depende”. Siempre debemos tener en cuenta el costo y el beneficio asociado a tener una acreditación. El costo puede ser económico, el tiempo de estudio que nos demande, etcétera. También debemos considerar el cargo

profesional al que apuntamos, debido a que, en ciertas organizaciones, es imprescindible tener un título para obtener trabajo. Puntualmente, en la seguridad informática se habla más de certificaciones que de títulos de grado, por ser estas más flexibles y estar más actualizadas. En caso de que queramos diferenciarnos del resto, y de acuerdo con el perfil profesional que busquemos, podemos optar por diferentes certificaciones. Algunas de ellas son **CISSP**, **Security+**, **CISA**, **CISM** y **CEH**, entre otras.

EN LA PRÁCTICA PROFESIONAL

Capacitarnos constantemente mantiene nuestros cerebros ágiles y receptivos a nuevos conocimientos y experiencias. A medida que pasa el tiempo, vamos a notar que nos es cada vez más fácil leer documentación técnica y entender cómo funcionan los sistemas. Incluso vamos a tener la capacidad de deducir cosas que no nos son explicadas, debido a la experiencia que iremos desarrollando y a que el diseño de los sistemas y las herramientas suele seguir ciertos patrones comunes, que se repiten en la mayoría de las soluciones. También es muy recomendable que constantemente probemos nuevos productos y tecnologías, aunque no vayamos a utilizarlos. Para conocer cuáles son las herramientas que tenemos a nuestra disposición, y cuáles son las nuevas capacidades que se nos ofrecen. Esto nos permitirá analizar futuras compras o implementar esas funcionalidades nosotros mismos. Estar al tanto de las últimas tendencias del mercado es un requisito excluyente para mantenernos como profesionales de elite.





Figura 6. *CISSP (www.isc2.org) es considerada como una de las credenciales de mayor representatividad en el ámbito de la seguridad informática a nivel mundial.*

Otro punto importante, que muchos profesionales dejan de lado, es el dominio del idioma inglés. Este es necesario para comprender la mayoría de la documentación existente sobre seguridad. Si tenemos problemas para dominar este idioma, estaremos muy limitados en cuanto a las fuentes de información de las cuales podamos nutrirnos. Es importante que contemos con la capacidad de leer en inglés, aunque podemos dejar de lado el hecho de hablar y escribir, tareas no tan necesarias para el estudio. De todos modos,

OTRAS FUENTES DE INFORMACIÓN

Para conocer más acerca de las certificaciones de seguridad más importantes, podemos visitar sus sitios web correspondientes: CISSP (www.isc2.org), CEH (www.eccouncil.org) y Security+ (www.comptia.org). También podemos obtener más información sobre las certificaciones más respetadas, así como consejos y precios de los exámenes, en www.portantier.com

lo más importante siempre será nuestra aptitud y nuestros conocimientos, más allá de cualquier título que podamos tener

También son valorables nuestra capacidad para resolver problemas, el hecho de poder brindar las mejores soluciones e implementar correctamente las medidas de seguridad, ya que esto nos diferenciará como profesionales de primer nivel. Tengamos en cuenta que contar con una certificación garantiza que tenemos nociones acerca de ciertos tipos de conocimientos, pero el no contar con una no quiere decir que no los tengamos.

METODOLOGÍAS DE TRABAJO

Como toda área de estudio en desarrollo, la seguridad informática ha ido mutando con el correr del tiempo. Fue necesario crear nuevas tecnologías específicas para la protección de los datos, con la misma frecuencia con la que se crean las tecnologías que estamos encargados de proteger. Pero, más allá de que podamos evolucionar constantemente generando nuevos mecanismos de defensa, es necesario que contemos con bases sólidas sobre las cuales podamos trabajar. Estas bases son las metodologías que utilizamos para realizar nuestras tareas; debemos pensar en ellas como los fundamentos de cada una de nuestras acciones.

Es preciso ubicar estos conceptos en un nivel amplio, sin ser específicos, sino más bien globales, para que nos marquen los lineamientos acerca de cómo debemos proceder. En las siguientes páginas analizaremos varias

Las certificaciones CISSP, CISA y CISM continúan siendo las más valoradas por el mercado latinoamericano

(Fuente: II Encuesta Latinoamericana de Seguridad de la Información ACIS 2010)

metodologías que podemos implementar para aumentar nuestra productividad y destacar-nos como profesionales de primer nivel.

DEFENSA EN PROFUNDIDAD

Como la seguridad informática es una ciencia tan innovadora y evolutiva, suele plantear nue-



Figura 7. El enfoque en capas nos permitirá organizar mejor los controles que implementemos y aumentar la seguridad de nuestra organización.



Figura 8. La NSA (www.nsa.gov) es la agencia criptológica del gobierno de los Estados Unidos. Es un excelente recurso de información, ya que constantemente se publican documentos de interés; es la desarrolladora del proyecto **SELinux**.

vas maneras de hacer las cosas. Pero existe una metodología implementada en todo el mundo, que nadie pone en discusión y siempre se promueve como la mejor: **la defensa en profundidad** apunta a implementar varias medidas de seguridad con el objetivo de proteger un mismo activo. Es una táctica que utiliza varias capas, en la que cada una provee un nivel de protección adicional a las demás. Como veremos más adelante, ninguna medida de seguridad puede ser perfecta, con lo cual es mucho mejor contar con varias medidas, cada una de las cuales cumplirá su papel. Esto hace que no tengamos una dependencia absoluta de una sola medida de seguridad, lo que nos permite la posibilidad de fallo y hace que sea mucho más complejo acceder a un sistema de forma no autorizada. Dicha estrategia ha sido formulada por la **NSA (National Security Agency)**, como un enfoque para la seguridad informática y electrónica.

En un principio, este concepto se utilizó como una estrategia militar que buscaba retrasar más

que prevenir el avance del enemigo, lo que permitía ganar tiempo, muy valioso en el campo de batalla.

Debemos implementar dichas medidas basándonos en el paradigma de **proteger, detectar y reaccionar**. Esto significa que, además de incorporar mecanismos de protección, tenemos que estar preparados para recibir ataques, e implementar métodos de detección y procedimientos que nos permitan reaccionar y recuperarnos de dichos ataques.

Es muy importante balancear el foco de las contramedidas en los tres elementos primarios de una organización: personas, tecnología y operaciones.

Personas: alcanzar un nivel de seguridad óptimo empieza con el compromiso de la alta gerencia, basado en un claro entendimiento de las amenazas. Este debe ser seguido por la creación de políticas y procedimientos, la asignación de roles y responsabilidades, la asignación de recursos y la capacitación de los empleados. Además, es necesario implementar medidas de seguridad física y control de personal con el fin de monitorizar las instalaciones críticas para la organización.

Tecnología: para asegurar que las tecnologías implementadas son las correctas, deben establecerse políticas y procedimientos para la adquisición de la tecnología. Es preciso implementar varios mecanismos de seguridad entre las amenazas y sus objetivos; cada uno debe incluir sistemas de protección y detección.

Operaciones: se enfoca en las actividades necesarias para sostener la seguridad de la organización en las tareas cotidianas. Este tipo de medidas incluye: mantener una clara política de seguridad, documentar todos los cambios efectuados en la infraestructura, realizar análisis de seguridad periódicos e implementar métodos de recuperación.

MUST KNOW

Desde el punto de vista del atacante, es mucho más difícil penetrar un sistema que cuente con varias medidas de seguridad, debido a que siempre existe la posibilidad de que una de ellas sea fácilmente saltada, aprovechando un error humano o alguna otra condición particular, pero habrá otras para protegerlo.

EL PRINCIPIO KISS

El **principio KISS** recomienda la implementación de partes sencillas, comprensibles y con errores de fácil detección y corrección, rechazando lo complicado e innecesario en el desarrollo de una solución. El origen de este acrónimo es la frase en inglés **Keep It Simple, Stupid** (que, traducido al español, significa: mantenlo simple, estúpido). Aunque, implementado en el área de seguridad, y para ser menos ofensivos, bien podríamos decir **Keep It Simple & Secure** (mantenlo simple y seguro). La idea detrás de esto corresponde a la certeza de que

“ las cosas
simples y fáciles
de entender suelen
tener mucha mejor
aceptación que las
complejas

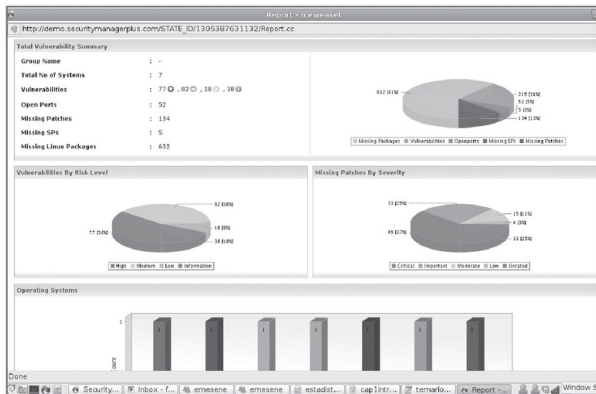


Figura 9. Muchas herramientas buscan mostrar de forma simple y gráfica el estado de la seguridad. Esto nos permite entender rápidamente cuál es nuestra situación actual para, luego, enfocarnos en los detalles.

Además, son mucho más fáciles de mantener, y esto es muy importante para las soluciones de seguridad, que muchas veces suelen caer en una excesiva complejidad, lo que termina en soluciones inentendibles e inmantenibles. Este concepto está relacionado directamente con el **principio de parsimonia**, según el cual:

“cuando dos teorías en igualdad de condiciones tienen las mismas consecuencias, la más simple tiene más probabilidades de ser correcta que la compleja”

Este principio es atribuido a Guillermo de Ockham, por lo que también es conocido como “La navaja de Ockham”.

Dicho principio puede (y debe) ser aplicado siempre y cuando nos encontremos en la situación de tener que elegir entre varios controles de seguridad que sean iguales o muy semejantes en cuanto a los beneficios que pueden aportarnos, pero diferentes en cuanto a su diseño y complejidad. Debemos prestar mucha atención a esto y no caer en implementar lo que nos sea más “fácil”, aun a costa de minimizar la funcionalidad o perder el foco de nuestro objetivo. Por lo tanto, es fundamental hacer un análisis completo de las soluciones disponibles a través de las metodologías que veremos más adelante, teniendo en cuenta que, a veces, la complejidad de una solución es la única forma de que esta satisfaga verdaderamente nuestras necesidades.

También hay que considerar los recursos con los que contamos para implementar un control de seguridad, tanto humanos, como de tiempo y dinero. Esto será fundamental para la toma de decisiones, debido a que una solución compleja, a la larga, puede ser imposible de mantener por una organización pequeña, en tanto que una demasiado sencilla puede no ser suficiente para los requerimientos de una organización grande.

EXPERIENCIA PROFESIONAL

En mis años de consultor me ha tocado conocer varios casos de implementaciones fallidas, que he tenido que solucionar. Una de las más memorables es la de una empresa que, como primera medida de seguridad para proteger sus puertos USB, decidió introducir pegamento en cada uno de ellos, bloqueándolos físicamente. Esta decisión había sido tomada por la gerencia, al ver que no necesitaban los puertos USB y que el pegamento era la forma más sencilla y económica para anular la posibilidad de acceso a ellos. Por desgracia, varios meses después, esa compañía se vio complicada al notar que muchos de los nuevos dispositivos que necesitaban utilizar requerían una conexión USB (como teclados, mouses y tokens de seguridad). En conclusión, la empresa tuvo que quitar el pegamento de los puertos USB (algunos quedaron igualmente inutilizables) e implementar

un herramienta para el controladores. Esto presentó un gasto de tiempo y dinero que se podría haber evitado desde un

re-



Figura 10. Guillermo de Ockham fue un fraile y filósofo inglés, oriundo de Ockham, de ahí su nombre. Para más información: http://es.wikipedia.org/wiki/Guillermo_de_Ockham.

DESDE ARRIBA HACIA ABAJO

Cuando se construye un edificio, el proyecto empieza con el diseño de los planos; luego, se construye la base y el resto del edificio, con cada puerta y ventana en su lugar, como está especificado en los planos. A continuación, los inspectores verifican que el edificio esté bien construido y que siga las indicaciones de los planos. ¿Notaron la cantidad de veces que aparece la palabra "planos"? ¡Es porque son muy importantes!

Los objetivos de una organización son los planos de un edificio. Deben estar bien definidos desde el principio, para que todo el programa de seguridad esté desarrollado en base a ellos



Muchas veces las organizaciones toman “el camino corto”, y empiezan a instalar aplicaciones de seguridad y a poner pegamento en los puertos USB para bloquearlos (sí, realmente algunos hacen eso). El problema no está en lo precario de aplicar el pegamento, sino en lo inútil de trabajar sin saber hacia dónde queremos ir.

Lo que debemos hacer es empezar por tener una idea amplia y poco específica de lo que queremos obtener. Luego, sobre la base de estas ideas, pasaremos a trabajar en los detalles de las tareas que vamos a realizar para alcanzar los objetivos fijados. El siguiente paso es desarrollar e implementar las guías, estándares y procedimientos que van a soportar las ideas generales escritas inicialmente. A medida que avanzamos en el proceso, vamos siendo cada vez más específicos, pero siempre

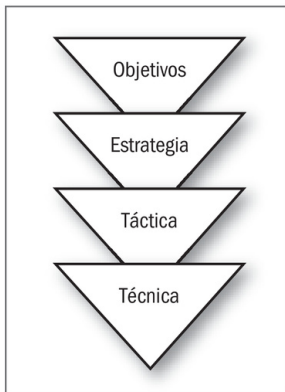


Figura 11. Una vez que tengamos los objetivos bien definidos, podemos pasar a desarrollar la táctica a través de la cual planeamos alcanzarlos. Hecho esto, estaremos en condiciones de pensar en las técnicas que utilizaremos.

con los objetivos principales en mente, hasta llegar a definir cada una de las configuraciones necesarias para cumplir con nuestras metas. Es importante trabajar con esta metodología, porque eso hace que no necesitemos realizar cambios drásticos ni rediseñar grandes partes de nuestros planes. Al principio, puede parecer que este enfoque lleva más tiempo y trabajo, pero, a medida que avancemos, notaremos que es el enfoque más sencillo, práctico y acertado.

“Un programa de seguridad debe estar soportado y dirigido por la alta gerencia, para luego ser distribuido hacia abajo en el árbol jerárquico, hasta alcanzar a toda la organización

Este enfoque se conoce como **desde arriba hacia abajo**. De esta forma, es fácil que toda la organización sea contagiada con los conceptos propuestos, y así se logre un trabajo armonioso y cooperativo. Este es el enfoque indicado si consideramos que la seguridad de la información debe ser prioridad dentro de los objetivos de la organización, que son definidos, como cualquier otro, por la alta gerencia.

LA SEGURIDAD EN LAS EMPRESAS

Las empresas, de forma consciente o inconsciente, han volcado sus procesos de negocio netamente a los sistemas de información. Siempre con el fin de volverse más productivas, ahorrar costos y poder realizar negocios en todas partes del mundo, cada una de las operaciones de una empresa se ha transformado en parte de una aplicación informática.

La información, que años atrás era almacenada en papel (el cual podía guardarse en un lugar conocido, leerse, copiarse y destruirse a mano), ahora se encuentra dispersa en forma de ceros y unos, dentro de varios medios de almacenamiento, como memorias USB, discos duros, dispositivos ópticos, y otros. Esto ha creado una amplia diversidad de fuentes de información, que nosotros estamos encargados de proteger. Dentro de las filas de una organización que se rige por un presupuesto, nuestros recursos para brindar protección y seguridad serán limitados. Algunas empresas asignan más capital a la seguridad informática que otras, pero lo cierto es que todos, en mayor o menor medida, nos encontramos limitados en cuanto a los recursos de que podemos disponer para realizar nuestras tareas.



Figura 12. Los pendrives USB han abierto nuevas formas de ataque, debido a que son un excelente hogar para todo tipo de virus. Además, son un medio muy utilizado para el robo de información.

Como buenos profesionales de la seguridad, debemos tener en cuenta las necesidades de la organización, con el fin de alinear las prácticas de seguridad con los objetivos de la empresa

Esto es imprescindible si pretendemos integrar la seguridad como uno de los procesos de negocio.

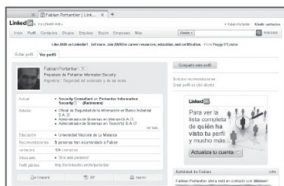


Figura 13. LinkedIn y otras redes sociales se presentan como un desafío para la seguridad, debido a que pueden ser utilizadas para trabajar, pero también, para difundir información confidencial.

LA SEGURIDAD COMO PROCESO DE NEGOCIO

Como vimos anteriormente, el compromiso con la seguridad debe partir desde lo más alto del árbol jerárquico de una organización: la alta gerencia. Para esto, es necesario que las personas encargadas de definir los rumbos de la empresa vean la seguridad como un proceso que no los obliga a gastar dinero, sino que les permite tanto ahorrarlo como ganarlo. Básicamente, ¿cuál es la diferencia entre ahorrar dinero y ganar dinero?

Si aseguramos nuestros sistemas de modo que no tengamos interrupciones de servicio, estaremos ahorrando el dinero que perderíamos al no poder trabajar. Si les demostramos a nuestros clientes un compromiso con la seguridad de sus datos y con brindar un servicio de primer nivel, estaremos ganando más dinero porque atraeremos más clientes y mantendremos contentos a los que ya tenemos. Estos son, simplemente, dos ejemplos de cómo podemos utilizar la seguridad informática con objetivos directamente relacionados con el negocio.

Las empresas ven como obstáculos de seguridad la falta de apoyo de la gerencia (15,21%) y la falta de entendimiento (18,47%)

(Fuente: II Encuesta Latinoamericana de Seguridad de la Información ACIS 2010)

Para todo profesional de la seguridad, es de suma importancia tener la capacidad de exponer estos conceptos ante los directivos de una empresa, con el objetivo de llamar su atención. Como cada persona habla su propio lenguaje, dependiendo de su área de especialización, es imposible que podamos convencer al gerente de marketing sobre las ventajas del nuevo sistema de protección de datos personales, si le marcamos que lo bueno del sistema es que está programado en Python y que usa una capa de abstracción que permite extender el sistema por medio de plugins que se desarrollan utilizando la API del fabricante. Seguramente, apenas escuche la palabra "Python", dejará de prestarnos atención.

Una situación muy distinta puede darse si le explicamos que tener un sistema de protección de datos personales permite asegurar a nuestros

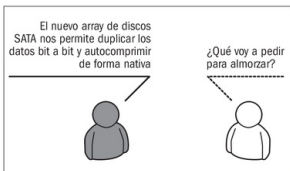


Figura 14. *Tengamos en cuenta con quién estamos hablando, y pensemos correctamente en qué decir y cómo hacerlo. De lo contrario, es muy probable que no nos presten la atención que deseamos.*

clientes que sus datos se encuentran protegidos por una tecnología muy avanzada, que garantiza que nuestra organización cuidará de ellos y de sus intereses. Siempre debemos hablar en el "lenguaje" de nuestro interlocutor; esta es una de nuestras tareas como verdaderos profesionales.

MUST KNOW

Debemos recordar que, cuando hablamos de recursos, no tenemos que considerar solamente el dinero; también debemos tener en cuenta los recursos humanos y los tiempos de los que disponemos, los cuales, muchas veces, terminan siendo factores tanto o más importantes que los recursos monetarios.

EN LA PRÁCTICA PROFESIONAL

Es una excelente idea que, antes de hablar con personas ajenas al ámbito de la seguridad informática, tengamos unos minutos para reflexionar acerca de qué ventajas debemos exponer. Ponernos en la piel de la otra persona y analizar sus necesidades nos permitirá conectarnos mejor con cada uno de los integrantes de la empresa.

Recordando estos consejos, podremos lograr que la seguridad informática sea vista en toda la organización como algo necesario, que no se hace por obligación sino por una necesidad, y que mantener nuestra empresa segura nos beneficia a todos.

MÉTRICAS DE SEGURIDAD

Partiendo de la base de que no podemos hablar de seguridad si no tenemos la capacidad de medir de alguna manera su estado, vemos que se torna necesario contar con una metodología que nos ayude a comprender en detalle nuestra situación actual y pasada. Siendo más específicos, es necesario que, por lo menos, podamos contestar a la pregunta básica: "¿cuánto hemos mejorado nuestra seguridad con respecto al año anterior?". El verdadero objetivo de hacernos esta pregunta es contar con una respuesta que pueda ser entregada a la alta gerencia, con el objetivo de asistirle en la toma de decisiones que marcarán el rumbo de la organización. Por lo tanto, las métricas que definimos y los valores que obtenemos tienen que poder ser expresados en un lenguaje entendible desde el punto de vista del negocio. Podemos tener grandes reportes con datos y vulnerabilidades identificadas, los cuales carecerán de sentido si no sabemos qué es aquello que queremos responder y cómo esto beneficia a la organización.

Lo cierto es que necesitaremos, al menos, dos tipos de métricas. La primera debe tener un enfoque técnico, y nos servirá para analizar minuciosamente en qué puntos podemos mejorar, qué vulnerabilidades debemos solucionar primero, qué medidas de seguridad están teniendo éxito, cuáles deben ser reemplazadas o modificadas, etcétera. Este reporte estará destinado a las áreas tecnológicas, y debe ser revisado por personal idóneo, que tenga la capacidad de proponer mejoras y adquirir nuevas soluciones.

El segundo reporte debe ser dirigido a la

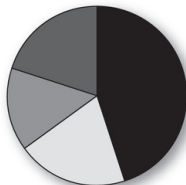
dirección de la empresa, y tendrá como objetivo mostrar un pantallazo general acerca de cuál es nuestra situación con respecto a la seguridad: en qué hemos mejorado, en qué debemos mejorar y si existen nuevas problemáticas que necesitamos resolver. También podemos incluir propuestas de inversión, ya sea de recursos tecnológicos, recursos humanos o capacitaciones al personal. También debemos tener en cuenta que no todo es medible, porque existen valores subjetivos de los cuales no podremos obtener gráficos ni valores concretos. Por ejemplo, en el caso de que nuestro sitio web sea atacado y modificado, la pérdida de credibilidad que sufrirá nuestra organización no será medible (aunque sin duda será algo muy negativo). Para resumir la importancia de las métricas, debemos recordar una frase que se aplica no solo a la seguridad, sino también a la gestión de cualquier proceso: "Si no lo puedes medir, no lo podrás gestionar".

MEJORA CONTINUA

El proceso de **mejora continua** es un concepto que pretende mejorar los productos, servicios y procesos en todos los niveles de una compañía. Al igual que los conceptos anteriores, este debe ser implementado como actitud constante por cualquier organización que desee alcanzar objetivos ambiciosos. Formalmente, los sistemas de gestión de calidad, las normas ISO y los sistemas de evaluación ambiental se utilizan para alcanzar objetivos relacionados con la mejora continua. Más allá de esto, no es necesario seguir estrictamente estas guías para entrar en un ciclo de mejoramiento permanente, pero son excelentes puntos de partida. En general, es posible conseguir una mejora continua reduciendo la complejidad y los puntos potenciales de fracaso; mejorando la comunicación, la automatización y las herramientas, y colocando puntos de control y salvaguardas para proteger la calidad de las operaciones de una organización. Más allá de

Información Técnica

Sistema	Vulnerabilidades
Web Server 1	5
Web Server 2	7
Database	3
Intranet	12
File Server	10
Access Server	8

Información Gerencial

que existen documentos y normativas relacionados con el proceso de mejora continua, debemos tomar este concepto por lo que es (un concepto), y aceptar que

“La metodología que nos lleve a un proceso de mejora continua será necesaria y debe ser bienvenida por la organización

Para esto, hay que seleccionar las metodologías que mejor se adapten a las necesidades particulares de cada entorno.

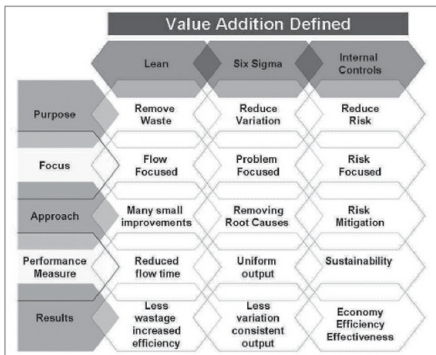
Figura 15. Sobre la base de la información técnica, generalmente obtenida de varias herramientas, debemos generar reportes sencillos, enfocados en la gerencia.

Debemos saber también que, así como no es posible alcanzar la perfección, tampoco es posible lograr un ambiente 100% seguro. Simplemente, esto es algo a lo que podemos aspirar a través de varios esfuerzos bien dirigidos. Pero cabe recordar que este es un trabajo constante, que nunca llega a un final, porque siempre está persiguiendo una perfección que no deja alcanzarse. Visto de otro modo: la perfección siempre intenta alejarse de nosotros. Depende de nuestras capacidades el hecho de que podamos seguirle el paso, y mantenernos siempre pisándole los talones.

Es imperativo que tengamos la capacidad de mantener los procesos de nuestra organización al nivel más simplificado posible (KISS) y que seamos capaces de medir los resultados dentro de una línea de tiempo (métricas). Haciendo esto, tendremos las herramientas necesarias para mejorar la calidad de nuestros procesos constantemente (mejora continua). La seguridad absoluta es algo imposible. Tendremos que aprender a vivir con eso. Una vez que

Figura 16. Seis

Sigma (o Six Sigma) es una metodología ampliamente utilizada para la mejora continua, que se vale de herramientas estadísticas para la caracterización y el estudio de los procesos.



hayamos asimilado esta idea, podremos empezar a pensar en acercarnos a la perfección, sabiendo que nunca lograremos alcanzarla. El trabajo arduo y constante nos llevará a perfeccionarnos, a mejorar nuestras capacidades de respuesta y a predecir los eventos que podrían causar un impacto negativo en nuestras organizaciones.

Esto es un entrenamiento que va más allá de un curso o de un título de grado: se consigue con la experiencia cotidiana y con la capacidad de mirar hacia atrás, para no volver a cometer los errores pasados, y aventurarnos a cometer errores nuevos. Siempre depende de nosotros ser excelentes profesionales.

PARA PONER A PRUEBA

1. ¿Cuáles son las ventajas y desventajas de la superespecialización?
2. ¿A qué hace referencia el principio KISS?
3. ¿Cuáles son las ventajas de implementar defensa en profundidad?
4. ¿Es posible lograr que una organización sea 100% segura? ¿Por qué?
5. ¿Por qué son importantes las métricas de seguridad?

CAPÍTULO 2

GESTIÓN DE LA SEGURIDAD

PARA APROVECHAR ESTE CAPÍTULO

» **REALIZAR** EL EJERCICIO DE IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES, AUNQUE SEA CON VALORES IMAGINARIOS, NOS SERVIRÁ COMO EXPERIENCIA.

» **DESCARGAR** LAS PLANTILLAS DE DOCUMENTOS DEL SANS INSTITUTE QUE SE MENCIONAN COMO REFERENCIA, LEERLAS Y ANALIZARLAS. NOS DARÁN UNA EXCELENTE IDEA DE CÓMO REDACTAR MUY BUENOS DOCUMENTOS.

» **ACCEDER** A LOS SITIOS WEB DE LAS ENTIDADES MENCIONADAS. TODAS CUENTAN CON EXCELENTE RECURSOS QUE NOS AYUDARÁN EN NUESTRO PROCESO DE CAPACITACIÓN CONSTANTE.

GESTIÓN DE LA SEGURIDAD

En este capítulo aprenderemos a:

Objetivo 1 Comprender el proceso de gestión de la seguridad informática.

Objetivo 2 Entender las responsabilidades que tiene cada persona dentro de la organización.

Objetivo 3 Saber cómo y por qué deben redactarse los documentos formales.

Objetivo 4 Identificar las amenazas, vulnerabilidades y riesgos con los que nos enfrentamos.

La gestión de la seguridad es un proceso amplio, que incluye muchísimas tareas de distinta índole, como la administración de riesgos, el mantenimiento de políticas, la clasificación de la información y la capacitación de los miembros de la organización. Por eso nos encontramos con una profesión tan apasionante, que demanda de nosotros una gran variedad de conocimientos. Dentro de ella, podremos encontrar varias especializaciones, cada una de las cuales puede tener un foco más técnico o más administrativo, pero que comparten los mismos fundamentos, los cuales debemos conocer a la perfección si queremos garantizar la elección e implementación correcta de las medidas de seguridad. La única diferencia que debe existir entre unos y otros profesionales es el porcentaje de contacto que tendrán con cada uno de los aspectos de la seguridad. Dado que un gerente pasará más horas de su jornada redactando y analizando políticas, y que

un administrador analizará configuraciones de sistemas y redes durante la mayor parte de su tiempo, ambos deben conocer en su totalidad las tareas por realizar. Para guiarnos en este proceso,

“es recomendable la metodología de gestión de riesgos informáticos del NIST, que se encuentra detallada en el documento SP 800-30

de aproximadamente cincuenta páginas. El texto está escrito de un modo sencillo y presenta una metodología que no requiere demasiado tiempo para poner en práctica. Está disponible para descarga gratuita en el sitio oficial de dicho instituto, y si bien no abarca todos los temas que intervienen en el proceso de gestión, es una excelente guía de referencia y consulta.

MUST KNOW

Para ser excelentes profesionales, debemos tener la capacidad de analizar todo el proceso de gestión de la seguridad, conociendo todas las tareas que se realizan, aunque sea de una manera superficial. Solo así podremos tener una visión global, que nos permitirá optimizar nuestras actividades para alcanzar los objetivos de la organización.

El **National Institute of Standards and Technology** cuenta con una división especializada en seguridad de la información, de la cual podremos obtener valiosísimos documentos que nos servirán como guía para nuestras actividades.

Para conseguir más información, podemos visitar su sitio web en **csrc.nist.gov**.

Otra metodología que puede ser de gran interés es **OCTAVE**, publicada por el **CERT Coordination Center**, de la **Universidad de Carnegie Melon**. Se trata de una metodología mucho más extensa, que cuenta con una versión para pequeñas y medianas empresas, conocida como **OCTAVE-S**. Aun así, esta última es mucho más grande que la **SP 800-30** del **NIST**. Como ambas metodologías son de libre descarga, queda en nosotros elegir cuál se adapta mejor a nuestras necesidades. Dicho instituto también ha desarrollado una certificación enfocada en la respuesta a incidentes de seguridad informática (**Certified Computer Security Incident Handler**).

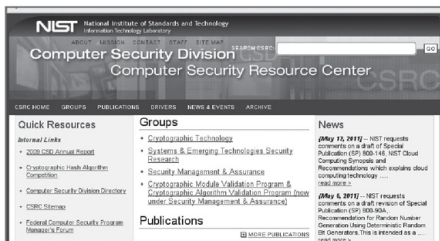


Figura 1. El National Institute of Standards and Technology es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.



Figura 2. En el sitio web del CERT, además de la metodología OCTAVE, podemos encontrar una gran cantidad de información y documentos de interés.

EL AUTOCONOCIMIENTO

La importancia de conocernos a nosotros mismos y saber exactamente a qué debemos temer, es la clave para tener éxito, no solo en la seguridad informática. Para remarcar la importancia de este tema, citaremos un fragmento del milenario libro **El arte de la guerra**, de **Sun Tzu**:

“Si conoces al enemigo y te conoces a ti mismo, no te pondrán en peligro ni cien batallas. Si no conoces al enemigo, pero te conoces a ti mismo, perderás una y ganarás otra. Si no te conoces ni a ti ni al enemigo, estarás en peligro en todas las batallas”.

“ Como observamos, conocernos a nosotros mismos y los peligros que rondan a nuestro alrededor es de vital importancia para obtener la victoria en la tarea de asegurar información

Es por eso que, antes de pensar siquiera en implementar medidas de seguridad, debemos tomar acciones para conocer a fondo nuestra infraestructura tecnológica. De este modo,

MUST KNOW

Muchas empresas pasan por alto la tarea de clasificar sus activos, pensando que ya conocen su infraestructura por el hecho de estar en contacto con ella constantemente. Este es un error muy común, pero grave. El primer paso, y requisito fundamental para la seguridad informática, es conocer exactamente qué tenemos y cuánto vale para nosotros.

podremos asignarles un valor a los activos que la componen y, así, definir nuestra prioridades y los recursos que vamos a invertir para proteger cada uno de ellos. Debemos recordar que la tecnología no es otra cosa que una herramienta que simplifica tareas y optimiza procesos. Por eso, el conocimiento de qué sistemas son importantes para la organización está ligado estrechamente a los procesos de negocio, los cuales están a cargo



Figura 3. *El arte de la guerra es un libro escrito por Sun Tzu que trata sobre estrategias militares. Ha sido no solo utilizado para fines bélicos, sino también aplicado a varias áreas de estudio, como la administración de empresas.*

de los directivos y gerentes. Así que, para determinar cuáles son los sistemas más importantes, tendremos que consultar a los altos mandos de la organización. Por supuesto, como analizamos anteriormente, las consultas a los directivos deben realizarse teniendo en cuenta el lenguaje de nuestro interlocutor, por lo que tendremos que hacerlas en una forma parecida a la siguiente:

- 1 ¿Cuáles son las funciones principales del negocio?
- 2 ¿Cuáles son las tareas más importantes dentro de la organización?
- 3 ¿Qué tareas no pueden interrumpirse?
- 4 ¿Qué tareas pueden ser interrumpidas durante muy poco tiempo?
- 5 ¿Qué espera de su infraestructura tecnológica?

Esto nos da una idea del tipo de preguntas que debemos realizar, ya sea a través de cuestionarios o de entrevistas personales. Con las respuestas que obtengamos, podremos verificar qué sistemas intervienen en cada uno de estos procesos y, así, determinar la criticidad que tiene cada activo para la organización.

Una vez que tengamos bien identificados los procesos de negocio críticos, debemos pasar a describir nuestra infraestructura tecnológica. Para esto, podemos entrevistarnos con los encar-

Solo el 33% de las empresas de Sudamérica cuenta con un inventario que detalla en qué lugares se almacena la información

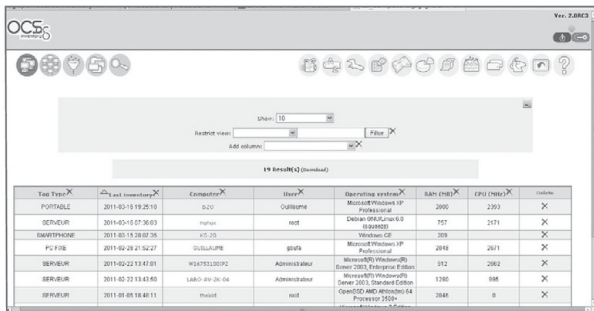
(Fuente: PWC Global State of Information Security Survey 2011)

gados de las áreas técnicas, que la mantienen y le dan soporte, ya sea personalmente o entregando cuestionarios, y analizando la documentación existente. Los datos importantes acerca de la infraestructura tecnológica serán:

- Usuarios (tanto los que brindan soporte como los que la utilizan).
- Topología de la red actual (diagramas de red).
- Flujo de información (conexiones con otros sistemas, internos y externos).
- Tareas del sector de IT (copias de seguridad, mantenimiento, replicación de datos, procedimientos para alta, baja y modificación de cuentas, etc.).

Figura 4. Arpwatch (<http://ee.lbl.gov>) es un software de código abierto que nos permite conocer los cambios de direcciones en los dispositivos de nuestra red. Es ideal para estar al tanto de nuevos equipos.





The screenshot shows the OCS Inventory web interface. At the top, there's a navigation bar with icons for various functions. Below it, a search bar contains the text 'ip: 10'. A table titled '19 Result(s) (download)' displays the following data:

Tag Type	Last inventory	Computer	User	Operating system	RAM (MB)	CPU (MHz)	Osinfo
PORTABLE	2011-03-16 19:25:10	D-20	Outlume	Microsoft Windows XP Professional	2000	2393	X
SERVEUR	2011-03-16 07:36:03	high	root	Debian GNU/Linux 6.0 (squeeze)	757	2171	X
SMARTPHONE	2011-03-16 20:07:26	HTC-20		Windows CE	200		X
PC IDE	2011-03-29 21:52:27	GULLAURE	gulla	Microsoft Windows XP Professional	2048	2671	X
SERVEUR	2011-02-22 13:47:01	W34783100192	Administrateur	Microsoft Windows Server 2003, Enterprise Edition	512	2062	X
SERVEUR	2011-02-22 13:43:50	LABO-SV-3K-04	Administrateur	Microsoft Windows Server 2003, Standard Edition	1780	686	X
SERVEUR	2011-03-05 18:40:11	thuid	root	OpenBSD AMD64 OpenBSD 6.4 Processor 380+	2048	0	X

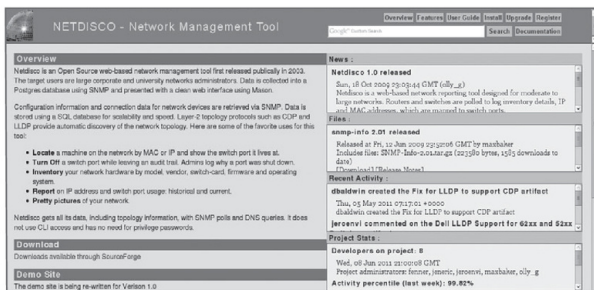
Figura 5. OCS Inventory es un software de código abierto que nos permite mantener actualizado un inventario de software y hardware. Esto nos será de mucha utilidad para generar el listado de activos al que luego vamos a asignar prioridades.

Y para cada uno de los dispositivos registrados debemos tomar nota de:

- » El propósito que cumple.
- » Hardware y software.
- » Configuraciones.

- » Información que almacena y/o procesa.
- » Personas que lo utilizan.

Es de vital importancia poder conectar las respuestas obtenidas de la gerencia con el inventario de activos de información, para determinar



The screenshot shows the Netdisco web interface. The main heading is 'NETDISCO - Network Management Tool'. Below it, there's a navigation bar with links like Overview, Features, User Guide, Install, Upgrade, Register, Search, and Documentation. The 'Overview' section describes Netdisco as an Open Source web-based network management tool. It lists features like:

- Locate a machine on the network by MAC or IP and show the switch port it lives at.
- Turn Off a switch port while leaving an audit trail. Admins log why a port was shut down.
- Inventory your network hardware by model, vendor, switch-card, firmware and operating system.
- Report on IP address and switch port usage. Historical and current.
- Pretty pictures of your network.

The 'Recent Activity' section shows a list of events, including:

- Netdisco 1.0 released: Sun, 18 Oct 2009 23:03:44 GMT by maxbaker
- snmp-info 2.01 released: Released at Fri, 12 Jun 2009 23:20:06 GMT by maxbaker
- dbaldwin created the fix for LLDP to support CDP artifact
- dbaldwin created the fix for LLDP to support CDP artifact
- jerome commented on the Dell LLDP Support for 62xx and 53xx

Figura 6. Netdisco (www.netdisco.org) es un software de código abierto que mantiene un inventario de los dispositivos de red existentes. Puede detectar nuevos dispositivos a través de SNMP, CDP y LLDP.

qué sistemas intervienen en el desarrollo de cada uno de los procesos de negocio identificados como críticos. Con todos estos datos a nuestra disposición, estaremos en condiciones de armar una tabla de activos y prioridades, la cual vamos a necesitar para completar las siguientes etapas del proceso de gestión.

ANÁLISIS CUALITATIVO VS. CUANTITATIVO

Al clasificar cada activo de la organización, nuestro principal objetivo será asignarle un valor, que refleje la importancia que tiene para nosotros. Para esto, existen dos tipos de análisis: el cuantitativo, en el que asignamos valores monetarios a cada uno de nuestros activos; y el cualitativo, en el cual nos basamos en valores de una escala (por ejemplo, de 1 a 10) para reflejar la importancia que le otorgamos a cada uno. Cada método tiene sus ventajas y desventajas. Podemos destacar, rápidamente, que los análisis cuantitativos son más exactos y más fáciles de entender por la gerencia, pero requieren un

trabajo muchísimo mayor y una gran cantidad de cálculos. Por su parte, los cualitativos se basan más en la percepción de necesidad que tienen las personas sobre un activo, lo que los vuelve mucho más sencillos de realizar y, si bien pueden ser no tan exactos, conforman una excelente fuente de información para la toma de decisiones. El tipo de análisis que vayamos a utilizar dependerá de cada uno de nosotros, según nuestros recursos y necesidades. En la mayoría de los casos, bastará con un análisis cualitativo, que nos permitirá conocer los valores de nuestros activos para poder asignarles prioridades.

Como expertos en seguridad, sacaremos más provecho a la lista ordenada de mayor a menor de los activos más importantes, que al valor de estos en sí

Cualitativo	vs.	Cuantitativo
Ventajas · Requiere cálculos simples. · Es fácil de mantener · Lleva menos tiempo de elaboración		Ventajas · Permite un mejor análisis costo-beneficio. · Es más entendible por la gerencia. · Puede automatizarse.
Desventajas · Los resultados son básicamente subjetivos. · No podemos obtener valores monetarios. · No existen estándares publicados.		Desventajas · Los cálculos son mucho más complejos. · Sin automatización, es muy complicado. · Se necesita mucho trabajo previo. · No existen estándares publicados.

Figura 7. En el diagrama analizamos brevemente las ventajas y desventajas de cada uno de los sistemas de valoración.

Dicha lista nos permitirá analizar sobre qué activos debemos trabajar primero y asignarles más recursos.

AMENAZAS Y VULNERABILIDADES

Cuando hablamos de gestión de la seguridad, es muy frecuente el uso de ciertos términos que, a veces, se intercambian incorrectamente y suelen prestarse a confusión. Aquí analizaremos con brevedad cada uno de ellos, tomando como ejemplo la situación de contar con una estación de trabajo que no tiene un antivirus instalado.

Vulnerabilidad: es una debilidad en algún software, hardware o procedimiento que puede permitir a un atacante realizar acciones que, normalmente, no tiene permitidas. En general, tiene como raíz la ausencia o la debilidad en uno

o más controles. En nuestro ejemplo, la vulnerabilidad es la ausencia de antivirus.

Amenaza: es cualquier peligro potencial sobre la información y/o los sistemas. La amenaza es alguien o algo que aprovecha una vulnerabilidad existente y la utiliza para provocar un daño. Puede ser de tipo no intencional (como errores humanos, tornados, terremotos, etc.) o intencional (hackers, empleados furiosos, etc.). En nuestro ejemplo, la amenaza es el virus.

Exposición: se refiere al impacto negativo que podríamos llegar a sufrir en caso de que la vulnerabilidad fuera explotada. El término "exposición" hace referencia al daño "probable". Cuando este daño se vuelve real, se lo conoce como "impacto". En nuestro ejemplo, estamos expuestos a que la estación se infecte y suframos la pérdida y/o corrupción de datos, además de su mal funcionamiento.

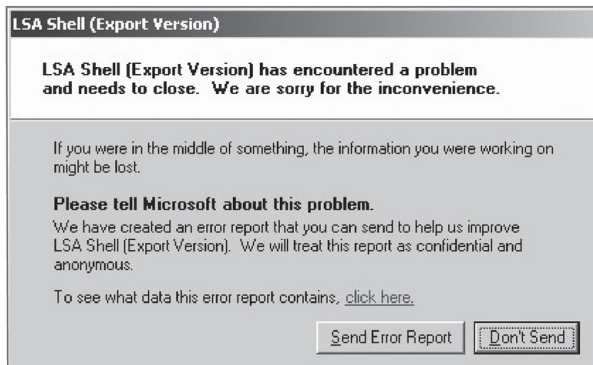


Figura 9. Podemos observar un mensaje emitido por un virus, que intenta tomar interacción del usuario al presentar características muy similares a las de los mensajes emitidos por el sistema operativo.

Riesgo: es el resultado de analizar la vulnerabilidad, la amenaza, la exposición y la probabilidad de explotación. En nuestro ejemplo, el riesgo es la probabilidad de que el virus infecte a la estación de trabajo. Suele categorizarse en bajo, medio o alto.

Contramida: se utiliza para mitigar los riesgos. Puede ser una configuración de software, un dispositivo o un procedimiento que elimine la vulnerabilidad o reduzca el riesgo de ocurrencia de que un agente de ataque explote dicha vulnerabilidad. En nuestro ejemplo, la contramida podría ser instalar un antivirus, acción que

MUST KNOW

En las organizaciones que se inician en el proceso de gestión de la seguridad, es recomendable utilizar un análisis cualitativo y asignar un único valor a la importancia de cada activo. Una vez hecho esto, tenemos la opción de volvernos más minuciosos y pasar a un análisis cuantitativo.

mitigaría el riesgo de una infección de virus.

El gráfico de la **Figura 11** explica la relación entre cada uno de estos conceptos.

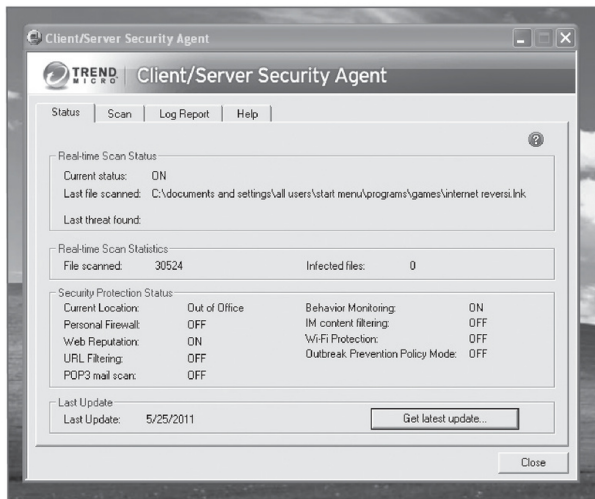


Figura 10. En la figura podemos ver en acción la herramienta antimalware TrendMicro, la cual es implementada como una medida de protección contra virus y otros tipos de malware.

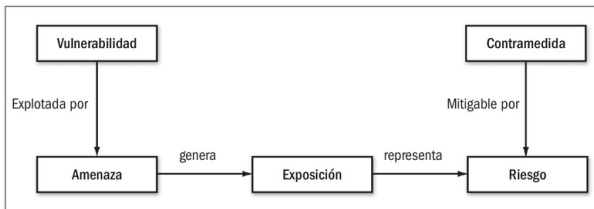


Figura 11. Proceso detallado acerca de cómo una vulnerabilidad puede causar problemas y cómo debemos mitigarla a través de contramedidas.

“Una vulnerabilidad puede ser explotada por una amenaza, hecho que generaría un cierto grado de exposición. Esto representa un riesgo, que es mitigable a través de contramedidas



Citando el ejemplo: “La ausencia de un antivirus en una estación de trabajo podría ser explotada por un virus, lo cual la expone a ser infectada y perder sus datos. Esto representa un alto riesgo para ella, que puede ser mitigado instalando un antivirus”. Aclarados estos términos, nuestra siguiente tarea es identificar cuáles son las amenazas que podrían impactar sobre nuestros activos. Debemos considerar amenazas tanto físicas como lógicas, y tanto intencionales como accidentales. Algunas de las más comunes son los hackers, los empleados descontentos y la competencia.

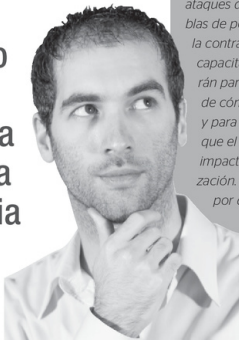
Para esto, podemos desarrollar una tabla con las amenazas más probables, a fin de contar con un listado que nos permita tener una buena visión acerca de cuáles son los peligros con los que nos enfrentamos. Es fundamental armar esta tabla con todas las amenazas

que se nos ocurran, para, luego, ir descartando las que sean muy poco probables o no se apliquen a nuestro entorno. Una vez que tengamos identificadas las principales amenazas, podemos empezar a trabajar sobre ellas, dejando las otras para siguientes repeticiones del proceso.

	Intencionales	No intencionales
Lógicas	• Hackers • Malware • Empleados descontentos	• Fallas de sistema • Empleados (errores de uso)
Físicas	• Ataques terroristas • Empleados descontentos	• Inundaciones • Terremotos • Fallas de hardware

Figura 12. En la imagen vemos una tabla con las posibles amenazas a las cuales se enfrenta una organización. Dependerá de cada situación particular si algunas de ellas se aplican o no, pero esta lista sirve para tener una idea de cómo confeccionar nuestra propia tabla.

“Lo importante es poner manos a la obra y ; luego, con el tiempo, iremos mejorando sobre la marcha y a partir de la experiencia



DEL EXPERTO

INCIDENTES DE SEGURIDAD

Tanto por experiencia profesional como a partir del resultado de varias estadísticas, podemos observar que una gran parte de los incidentes de seguridad son iniciados a través de accidentes, fallas o acciones no intencionales. Estos errores son muy comunes, sobre todo, por parte de usuarios inexpertos o en entornos en los que se realizan tareas muy complejas. Por lo tanto, debemos considerar que este tipo de acciones es tan importante como los ataques de hackers, y ubicarlas en las tablas de posibles amenazas. En estos casos, la contramedida más efectiva es realizar capacitaciones constantes, que servirán para entrenar a los usuarios acerca de cómo deben utilizar los sistemas, y para generar conciencia acerca de que el uso inadecuado de estos puede impactar negativamente en la organización. Además, debemos esforzarnos por que los sistemas implementados sean intuitivos y que adviertan al usuario antes de permitirle realizar acciones que podrían causar daños en el sistema.

Una vez que hayamos completado la tabla de amenazas, procederemos a investigar qué vulnerabilidades tenemos en nuestros sistemas. Ya sea a través del análisis minucioso de las configuraciones, el uso de herramientas automatizadas o cualquier otro método, obtendremos una lista de cada uno de los activos, con las vulnerabilidades que presenta. Es necesario emplear varios métodos para recabar este tipo de información, como analizar configuraciones, leer manuales y utilizar herramientas automatizadas, pero debemos saber que es necesario unificar estos datos, para trabajarlos de manera adecuada.

Para poder hacer uso de toda la información recolectada, deberemos ordenarla con el fin de poder realizar comparaciones y filtrados. Esto puede lograrse a través de herramientas especializadas, la creación de alguna pequeña

Figura 13. En la imagen vemos un listado de vulnerabilidades conocidas por activo, y las amenazas que podrían aprovecharlas para causar daños.

Activo	Vulnerabilidad	Amenaza probable
Estaciones de trabajo	• Fallas de antivirus • Puertos USB sin restricciones • Usuario Guest habilitado	• Malware • Usuarios descontentos • Hackers
Servidores	• Firewall deshabilitado • Sistema operativo desactualizado • Sin copias de respaldo de los datos	• Hackers • Hackers • Malware • Usuarios descontentos - Falla de hardware
Router externo	• Telnet habilitado • Falta de redundancia de hardware • ACL No definirá	• Hackers • Falta de hardware • Hackers

RECOMENDADOS

Algunas de las herramientas gratuitas que podemos utilizar para automatizar la búsqueda de vulnerabilidades son: **OpenVAS** (www.openvas.org); **Nexpose Community Edition**, de los mismos creadores de **Metasploit Framework** (www.rapid7.com); y **Microsoft Baseline Security Analyzer**, que sirve solo para plataformas **Microsoft** (www.microsoft.com).

herramienta con una base de datos relacional o haciendo un uso exhaustivo de planillas de cálculo. Lo importante de contar con una tabla de activos con vulnerabilidades explotables es que nos garantiza la capacidad de asignarles prioridad a aquellos que corren más peligro. Utilizaremos esta tabla en el siguiente paso.

Como final del proceso de identificación, obtendremos una tabla con los niveles de riesgo que tiene cada activo, sobre la base de cada una de las vulnerabilidades que posee. Con esto, podremos

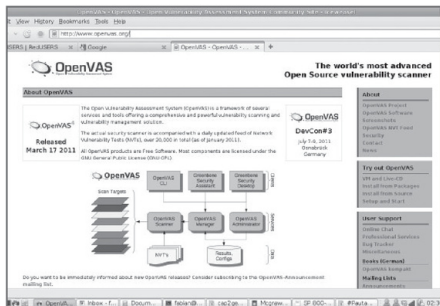


Figura 14. Este proyecto de código abierto está basado en el código de Nessus e intenta llenar el vacío que este dejó cuando pasó a ser totalmente software privativo. Es un excelente proyecto que cuenta con muchos usuarios y posibilidades de integración con otras herramientas. (www.openvas.org).

identificar rápidamente a qué acciones dar prioridad y recursos cuanto antes. Este tipo de tablas requiere una buena cantidad de cálculos matemá-

ticos (sobre todo, cuando disponemos de muchos activos). Es por eso que es ampliamente recomendable automatizar el proceso de algún modo.

Activo	Valor	Vulnerabilidad	Amenazas	Exposición	Probabilidad	Riesgo	Total Vuln
Servidor de archivos	5	Sin copias de seguridad	• Falta de hardware	5	3	75	145
			• Empleados (error de uso)	2	3	30	
			• Empleados descontentos	2	2	20	
Servidor de correo	5	• Software desactualizado • Sin copias de seguridad	• Hackers	4	3	60	60
			• Falta de hardware	5	3	75	75
Estaciones de trabajo	3	• Sin antivirus • Sin copias de seguridad	• Malware	4	5	60	60
			• Falta de hardware	5	2	30	30
Impresoras y escáneres	1	Admin sin password	• Usuarios descontentos	4	2	8	8

Escala de valores: Muy alta (5), Alta (4), Media (3), Baja (2) y Muy baja (1).

Figura 15. En la tabla podemos ver que la mayor necesidad es la de implementar un sistema de copias de seguridad para el servidor de archivos, que también podríamos utilizar para el servidor de correo. Además, habrá que instalar antivirus en las estaciones de trabajo y actualizar el servidor de correo. Las fórmulas aquí utilizadas son muy útiles y recomendables para un análisis cualitativo.

IMPLEMENTACIÓN DE CONTROLES

Una vez que tenemos identificados los riesgos, debemos hacer algo con ellos. En caso contrario, todo el esfuerzo realizado hasta el momento será en vano.

Así que tenemos que elegir cómo vamos a reaccionar ante cada uno de los riesgos y, para eso, necesitamos hacer un análisis de costo/beneficio a fin de determinar cuál será la mejor manera de actuar en cada caso. Podemos optar entre cuatro posibilidades, que son:

Mitigar: implementar medidas para reducir o eliminar un riesgo. Por ejemplo, para reducir el riesgo de una infección por virus, podemos instalar un software antivirus.

“No podemos, simplemente, barrer los riesgos debajo de la alfombra y hacer como si nada hubiera sucedido

Figura 16. La encuesta realizada por PWC en 2011 muestra los cambios en los motivos de inversión en seguridad informática de los últimos cuatro años.

PWC Global State of Information Security Survey 2011					
Motivos de inversión en seguridad informática					
Motivo / Año	2007	2008	2009	2010	Diferencia
Requerimiento del cliente	34%	31%	34%	41%	+21%
Práctica común de la industria	42%	37%	34%	38%	-10%
Posible impacto en los ingresos	30%	27%	26%	27%	-10%
Juicio profesional	45%	46%	40%	40%	-11%
Reducir el índice de riesgo	36%	31%	31%	30%	-17%
Evitar responsabilidades legales	49%	40%	37%	38%	-22%
Marco regulatorio o legal	58%	47%	43%	43%	-26%

Transferir: para transferir un riesgo a otra organización, generalmente podemos contratar un seguro para el activo que queremos proteger. Por ejemplo, para transferir el riesgo de que un dispositivo sufra una falla de hardware, podemos extender su garantía, y así asegurarnos un reemplazo de partes. Obviamente, esto no nos protege de una pérdida de información o de caídas de servicio, por lo cual debemos tener mucho cuidado al analizar qué riesgo estamos transfiriendo.

Evadir: cuando hablamos de evadir un riesgo, estamos haciendo referencia a eliminar la fuente que lo produce.

Esto quiere decir que preferimos dejar de utilizar un activo o proceso con tal de no sufrir los riesgos asociados a él. Por ejemplo, para evadir los riesgos que conlleva el uso de software de mensajería instantánea, podemos optar por bloquear su implementación.

Aceptar: este es el último recurso y debe ser utilizado solo cuando no podamos optar por ninguna otra alternativa. Cuando hablamos de aceptar un riesgo, estamos diciendo que tendremos que convivir con él, porque no resulta rentable implementar medidas de seguridad, pero de todos modos necesitamos la fuente que lo produce. Debemos tratar de mantener los riesgos aceptados en la menor cantidad posible. De todas estas opciones, siempre debemos tener en mente la mitigación como primera medida. Y solo cuando esta sea impracticable o ineficiente, deberemos considerar alguna de las otras mencionadas anteriormente.

Recordemos que los riesgos van a estar ahí, aun cuando intentemos mirar hacia otro lado, así que es mucho mejor hacerles frente de manera temprana, que después sufrir las consecuencias de no haberles dado la importancia que se merecían.

EN LA PRÁCTICA PROFESIONAL

Cuando aceptamos un riesgo, esto implica que alguien debe hacerse responsable de esa decisión y de las consecuencias que pueda llegar a traer haberlo aceptado. Es por eso que se deben considerar cuidadosamente las otras tres alternativas, antes de aceptar un riesgo. Si, a pesar de todo, se decide aceptarlo, es ampliamente recomendable exigir la firma de un documento por parte de la gerencia para cada caso específico. Esto permite dejar en claro los peligros a los cuales nos exponemos por hacer esto, y nos da la posibilidad de no caer en faltas que, luego, pueden ser muy perjudiciales para nuestro trabajo. También debemos recordar que la decisión de no invertir recursos en mitigar un riesgo, y exponer a la organización a la posibilidad de sufrir un impacto negativo, debe recaer pura y exclusivamente en la alta gerencia, por ser esta la única verdaderamente capacitada para tomar este tipo de decisiones, que, en la mayoría de estos casos, dependen de motivos económicos.



	Mitigar	Evadir	Transferir	Aceptar
Ventajas	· Permite un buen balance entre seguridad y funcionalidad. · Nos permite tener un mejor control. · Es la solución más personalizable. · Es la solución mejor vista en las auditorías.	· Suele ser una opción económica. · Puede ser de rápida implementación.	· Permite resolver rápido un problema.	· Es la opción más económica.
Desventajas	· Puede requerir investigación y adquisición de soluciones. · Puede tardar bastante tiempo en implementarse.	· No siempre es aplicable. · Podría hacernos perder funcionalidad.	· No siempre podemos hacerlo. · Puede tener un costo muy elevado.	· Al final, puede ser la más costosa. · En cierta forma, nos estamos dando por vencidos. · No siempre podemos hacerlo. · No es bien visto en las auditorías.

Figura 17. La tabla muestra una comparativa de las cuatro opciones que tenemos para lidiar con los riesgos, destacando las principales ventajas y desventajas de cada una.

POLÍTICAS Y OTROS DOCUMENTOS

Como analizamos en páginas anteriores, es necesario contar con un enfoque que va desde arriba hacia abajo, empezando por la alta dirección y bajando por todos los niveles jerárquicos. Este enfoque será menos específico en los niveles más altos, y aumentará su complejidad y sofisticación a medida que vayamos descendiendo. Es preciso tener en cuenta que la seguridad de una organización va muchísimo más allá de una regla en un firewall o de la configuración de un sistema de prevención de intrusos. Incluso, si bien estas son cuestiones que afectan a la seguridad, terminan siendo el resultado de un análisis que se inicia al escribir los documentos que servirán como guía para este tipo

de tareas. A continuación, analizaremos los distintos tipos de documentos con los que debemos contar, y daremos recomendaciones al elaborar cada uno de ellos.

POLÍTICAS

Son los documentos que explican las bases sobre las cuales la organización realiza sus tareas y busca cumplir sus objetivos. No tratan ningún tema en profundidad; al contrario, son una referencia a la misión y la visión a través de las cuales debe guiarse cada uno de los miembros. Tienen que estar escritas o, por lo menos, avaladas por la alta gerencia, debido a que explican la postura de la organización con respecto a la seguridad, y están basadas en los objetivos del negocio. También se deben tener presentes las leyes, los estándares y las reglamentaciones a los cuales la organización debe atenerse.

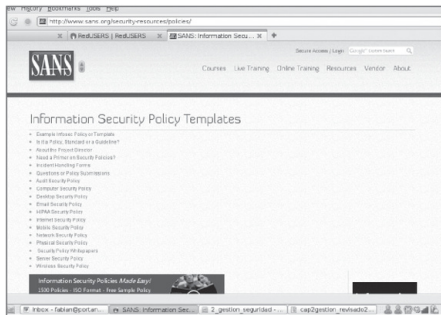


Figura 18. En el sitio web del SANS Institute podemos encontrar plantillas y guías que nos harán mucho más fácil la redacción de nuestros documentos. Aunque están en inglés, son un excelente punto de partida (www.sans.org/security-resources/policies).

MUST KNOW

Si esperamos que los empleados de una organización sigan al pie de la letra lo que dicta la política de seguridad, es necesario que hagamos accesible este documento a todos ellos, para que tengan la posibilidad de consultarlo cuando lo crean oportuno. También es muy recomendable que cada miembro de la organización acepte formalmente esta política.

Cada vez que la organización es modificada de alguna manera significativa, dichas políticas deben ser revisadas y cambiadas de forma acorde. También deben ser periódicamente revisadas para realizar las optimizaciones o correcciones correspondientes. Por eso, debemos escribirlas de manera generalizada, con el objetivo de no tener que modificarlas constantemente. Es recomendable que estos documentos estén redactados en forma sencilla y fácilmente entendible, para ser usados como punto de referencia por cualquier empleado de la organización. Es



Figura 19. En el sitio web del Center for Internet Security encontraremos, entre otras cosas, estándares recomendados para la configuración de nuestros sistemas operativos y dispositivos de redes (www.cisecurity.org).



Figura 20. Debemos respetar el orden en el cual generamos los documentos que guiarán nuestras tareas. Es un proceso lineal, en el cual cada documento se basa y nutre de los contenidos del anterior. Este orden nos ahorrará tiempo y nos permitirá desarrollar documentos de calidad.

MUST KNOW

Es una buena idea tomar las bases de normativas, estándares y recomendaciones ya avalados por entidades reconocidas para formular nuestros documentos. Esto nos permitirá disponer de contenido ampliamente revisado y desarrollado por expertos en la materia. Luego, podremos adaptarlos a las necesidades particulares de nuestra organización.

preciso remarcar la importancia que tienen y aclarar siempre las obligaciones de cada uno de los empleados, utilizando el modo imperativo (términos como "tiene/debe" en vez de "tendría/debería").

Cada uno de los empleados debe saber que esta política explica lo que la organización espera de ellos. Por consiguiente, la violación a los conceptos que dicha política explica, podría (y debería) implicar la aplicación de sanciones.

Si bien pueden existir varias políticas que cubran

aspectos específicos, la principal y más general suele ser llamada "política de seguridad de la información". Otras podrían estar destinadas a temas como: "uso de Internet y correo electrónico", "información confidencial", etc. Como las políticas deben escribirse desde un punto de vista global, es necesaria la independencia de cualquier tecnología o producto específico.

ESTÁNDARES

Estos documentos explican en qué forma van a ser alcanzados los objetivos propuestos por la organización en cuanto a aspectos de seguridad. Dictan de qué manera deben ser encarados los problemas y cómo tomar las decisiones. Muchas veces, suelen ser documentos generados por entidades externas y que son tomados por las organizaciones, ya sea en parte o en su totalidad. En estos documentos podemos empezar a hablar de tecnologías específicas

Figura 21. La tabla muestra las principales características de cada uno de los distintos documentos aquí mencionados.

Políticas

- Basadas en la visión y misión de la empresa.
- Redactadas o avaladas por la alta gerencia.
- Independientes de cualquier tecnología o producto.

Estándares

- Reflejan las tácticas de la organización.
- Hablan de tecnologías, pero no de productos.
- Pueden estar basados en estándares externos.

Procedimientos

- Datallan paso a paso cómo se realizan las tareas.
- Son específicos en cuanto a productos y versiones.
- Deben ser actualizados con frecuencia.

(algoritmos de encriptación, sistemas operativos, arquitecturas de hardware, etc.). Pero debemos hacerlo de un modo general, sin adentrarnos en el nombramiento de versiones específicas ni en otros detalles que dejaremos para los siguientes documentos. Con este tipo de documentos vamos a reflejar las tácticas de la organización, que estarán derivadas de la estrategia (lo que reflejan las políticas). Es importante que prestemos mucha atención al redactar un estándar o tomar uno externo, debido a que necesitaremos verificar que este se encuentre alineado con la política y que sea una buena base para la redacción de los procedimientos.

PROCEDIMIENTOS

Derivan de los estándares, y son los documentos que se encuentran en el nivel más práctico de todos. Esto significa que van a ser bien detallados, como guías paso a paso, que expliquen cómo realizar las tareas.

Son los documentos que más se modifican, debido a que la tecnología suele cambiar, y las nuevas versiones de los productos que utilizamos seguramente se instalarán y administrarán de manera diferente de sus predecesores.

En este caso debemos ser lo más específicos posible, pensando en que un procedimiento debería permitir que una persona que no contara con una vasta experiencia realizara la tarea mencionada sin mayores inconvenientes. Esto también nos servirá de gran ayuda cuando necesitemos hacer un reemplazo, debido a la partida de un integrante, o a una ausencia, ya sea por vacaciones, enfermedad o cualquier otro motivo.

La tarea de mantener actualizados los procedimientos debe ser constante, y tenemos que asegurarnos de marcar bien cuál es la última versión del documento, debido a que, en muchas ocasiones, puede ocurrir que existan varias versiones, y esto generará muchísima confusión. Tanto para los procedimientos, como para los

estándares y las políticas, consideremos utilizar un repositorio conocido por todos los miembros de la organización, que esté bien ordenado y nos permita realizar controles de acceso. Esto nos dará la posibilidad de optimizar las tareas de mantenimiento, evitará confusiones y garantizará un mejor seguimiento con el correr del tiempo. Además, muchos procedimientos podrían llegar a contener información que no es recomendable que sea conocida por todos los integrantes de la organización. Por lo tanto, un repositorio o servidor de archivos nos permitirá definir permisos granulares, con el objetivo de restringir el acceso de los empleados únicamente a los documentos que precisan para realizar sus tareas correctamente.

RESPONSABILIDADES

La seguridad informática tiene mucho que ver con las responsabilidades, debido a que nuestra tarea es proteger.

A veces nos olvidamos de esto porque todo marcha bien, y seguramente lo recordaremos cuando haya algún problema y alguien tenga que "pagar los platos rotos". Una de nuestras principales tareas es no solo ser responsables de nuestros actos, sino también recordarles a los demás que también tienen responsabilidades que cumplir.

MUST KNOW

*El término **due diligence** es el acto de investigar y entender los riesgos con los cuales se enfrenta una organización. Por su parte, **due care** implica que la organización demuestra un compromiso con la seguridad, implementando medidas, redactando documentos y generando conciencia en los empleados. Estos dos términos son muy importantes.*

“Después de todo, no podemos pretender que una persona actúe de forma responsable si desconoce cuáles son sus responsabilidades que la organización espera de ella

Figura 22. Algunas normativas exigen una determinada estructura básica para los equipos de seguridad, como la que podemos ver en la figura. Dentro de ella, existen distintos roles, para la separación de tareas.



Figura 23. El sitio web de Inteco (www.inteco.es) es un excelente recurso de información para que nuestro equipo de seguridad se mantenga actualizado.



Desde la alta gerencia, hasta los empleados de más bajo rango, todos los integrantes de la organización tienen distintas obligaciones que cumplir y, también, son responsables de velar por los intereses comunes. Esto debe ser puesto en claro desde un primer momento, para evitar confusiones y malos entendidos que más tarde puede ser catastróficos, tanto para la empresa como para las personas que la componen.

En última instancia, la responsabilidad de cada una de las acciones que lleva a cabo una organización recae sobre sus directores. Es por eso que debemos tener en cuenta que, más allá de los premios y castigos que puede recibir un empleado, la mayoría de las veces quienes tienen que responder ante la ley son los directores.

EL EQUIPO DE SEGURIDAD

Para lograr una implementación correcta de las medidas de seguridad, es necesario que cada organización cuente con un equipo designado a

MUST KNOW

PC Security Test es una interesante aplicación desarrollada para analizar la seguridad. Este programa se encarga de realizar un análisis muy rápido de la configuración general del sistema para después entregarnos un completo informe con la descripción de cada uno de los elementos encontrados. Está en idioma español y podemos descargarlo desde www.pc-st.com/es/index.htm.

mantenerlas. Dependiendo del tamaño de cada entidad, de sus capacidades económicas y sus políticas de seguridad, el equipo puede estar conformado por una (algo bastante solitario y decepcionante) o varias personas. El objetivo de este equipo es coordinar y mantener las políticas, estándares, procedimientos y medidas de seguridad aplicadas, así

como también realizar periódicamente revisiones y auditorías, y aconsejar a la alta gerencia.

Además, este equipo debe contar con colaboradores designados de cada una de las principales áreas de la organización. Como tarea de tiempo parcial, ellos intervendrán en la asistencia a reuniones periódicas, el reporte de estado, y otros aspectos. El objetivo último de este equipo es garantizar que las medidas de seguridad se implementen de manera efectiva.

Si analizamos algunas de las normativas y las formas de procedimiento de las empresas más grandes de los Estados Unidos y varios países de Europa, veremos que existen no uno, sino varios equipos relacionados con la seguridad informática, como puede ser el de gestión de riesgos, el de seguridad informática y el de respuesta a incidentes, entre otros.

Esto es algo que no todas las empresas pueden permitirse y, principalmente, que no todas las



Figura 24. La oficina de seguridad del internauta es un excelente sitio para que los usuarios obtengan información acerca de cómo protegerse en Internet. También es un muy buen recurso para complementar las capacitaciones que deben brindarse dentro de la organización.

empresas necesitan. Es por eso que tenemos que analizar cuáles son nuestras verdaderas necesidades y crear equipos sobre esa base, teniendo en cuenta que una cantidad excesiva de equipos nos traerá problemas de coordinación y burocracias innecesarias.

La mayoría de las empresas puede cumplir todos sus requerimientos con un equipo dedi-

cado exclusivamente a la seguridad informática y con colaboradores de cada uno de los departamentos. También debemos asegurarnos de que dicho equipo reciba capacitaciones constantes, y cuente con los recursos imprescindibles para llevar a cabo sus tareas y mantenerse al tanto de lo que pasa en el mundo de la tecnología.

EN LA PRÁCTICA PROFESIONAL

El Departamento de Recursos Humanos es el nexo entre los miembros de la organización y la organización en sí misma. Como interviene en los procesos de contratación, modificación de roles y despido, es imprescindible que se mantenga un contacto fluido entre este departamento y el equipo de seguridad informática. De ellos depende que este equipo esté al tanto de las cosas antes de que sucedan, para poder tomar las acciones correspondientes en tiempo y forma. Esto es de vital importancia en los casos de despido, en los cuales se deben bloquear inmediatamente todos los permisos de la persona despedida, incluso, antes de que esta se entere de que dejará de pertenecer a la empresa. Esto le impedirá realizar cual-

quier acción malintencionada, debido al descontento que puede producirle la situación. En los casos de nuevas contrataciones, el aviso previo al equipo de seguridad garantiza que todos los accesos estén concedidos a tiempo, para que el nuevo integrante pueda iniciar sus tareas lo antes posible.



El 50% de las empresas asegura que su personal de IT no tiene el suficiente conocimiento sobre seguridad informática

(Fuente: Symantec 2010 SMB Information Protection Survey)

CAPACITACIÓN AL PERSONAL

Es bien sabido que el personal técnico y relacionado con la seguridad informática debe recibir un entrenamiento constante, para estar actualizado en cuanto a las últimas medidas de seguridad y las nuevas tendencias. Pero no siempre se tiene en cuenta que la seguridad informática es un tema que abarca a las organizaciones en su totalidad, y es por eso que cada uno de sus miembros debe tener las nociones y los fundamentos de seguridad bien presentes.

Muchas de las vulnerabilidades e incidentes de seguridad ocurren por negligencia de los usuarios. Pero esto no quiere decir que la culpa sea de los propios usuarios, sino más bien de los responsables de la organización, que no vieron la importancia de capacitarlos correctamente.

Es por eso que debemos tener en cuenta la necesidad de desarrollar un programa de capacitaciones dirigido específicamente a los usuarios finales, para educarlos y que sepan exactamente cómo comportarse y reaccionar ante cualquier actividad sospechosa.

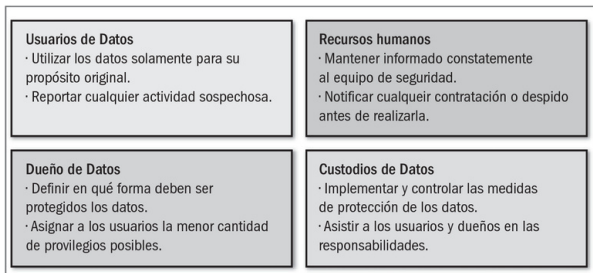


Figura 25. En el gráfico podemos ver las responsabilidades más importantes de cada uno de los roles explicados. Debemos tener en cuenta que absolutamente todos los integrantes son usuarios de datos, aun cuando tengan otros roles adicionales (recursos humanos, dueños o custodios de datos).

La forma más efectiva de brindar estas capacitaciones es ponerlas a disposición de los usuarios de manera online, y hacer que, luego, ellos tengan que rendir un pequeño examen, de preguntas al azar, para demostrar que han prestado atención al contenido visto y estar seguros de que lo han entendido. También es bueno enviar noticias y consejos de seguridad periódicamente, no tanto con la esperanza de que los empleados los sigan al pie de la letra, sino para que nos tengan presentes en todo momento y sepan que estamos para ayudarlos.

Más del 70% de las empresas invierte menos del 5% del presupuesto de seguridad en capacitación a usuarios

(Fuente: CSI Survey 2009)

DUEÑOS, CUSTODIOS Y USUARIOS DE DATOS

Si bien la información en su totalidad pertenece a la organización, es necesario que, para protegerla correctamente, sean asignados los roles de dueños y custodios. Esto es así porque tiene que existir alguien que dicte las formas en las cuales se van a proteger los datos, y que se haga responsable por lo que se hace con ellos. En general, es una buena idea definir a los dueños de datos basándonos en el departamento al cual pertenece dicha información. Por ejemplo, para los datos relacionados con el marketing, podemos señalar rápidamente al Gerente de Marketing como dueño. Esto hace

MUST KNOW

*Un intruso en un datacenter, incluso no pudiendo acceder a sistemas operativos y consolas de operación, puede atentar contra la **disponibilidad** desconectando elementos de red y servidores, o realizar otras acciones maliciosas, como el apagado de sistemas de refrigeración.*

que dicha persona tenga ciertas obligaciones y derechos por sobre esa información, que deben ser impuestos por la alta gerencia. Así serán respetados al pie de la letra y quedará clara la importancia de este tipo de responsabilidades. La persona que tenga el rol de dueño de datos estará encargada de comunicar al equipo de seguridad informática cómo debe ser protegida la información, y de explicar qué importancia tiene esta para la organización y las tareas que su departamento realiza. Además, podrá definir qué usuarios accederán a dichos datos y con qué permisos.

Los custodios de datos serán miembros del equipo de seguridad informática. Estarán encargados de asegurar que la información sea tratada y protegida de acuerdo con lo solicitado por sus dueños. También verificarán que los controles funcionen correctamente y que no se violen las políticas de seguridad definidas. Además, se ocuparán del mantenimiento de los permisos asignados a los usuarios, eliminando los que corresponda cuando alguien deja la organización, y verificando que se quiten los que ya son innecesarios cuando alguien cambia de sector o se modifica su rol en la empresa.

Por otra parte, los usuarios también tienen una responsabilidad muy importante, que es la de utilizar los datos en forma correcta y sin malas intenciones, cumpliendo con lo que dictan las políticas de seguridad, sin difundir datos confidenciales ni realizar ninguna acción que pudiera perjudicar de alguna manera a la empresa. También tienen la responsabilidad de denunciar cualquier comportamiento sospechoso que pueda tener alguno de sus compañeros.

El hecho de que todos y cada uno de los miembros de la organización cumplan correctamente con sus responsabilidades es una de las bases más importantes para poder garantizar la protección de la información.

PARA PONER A PRUEBA

1. ¿Cuáles son las ventajas y desventajas del análisis cualitativo?
2. ¿Cómo se relaciona el nivel de riesgo con las amenazas y las vulnerabilidades?
3. ¿Cuáles son las cuatro formas de responder ante un riesgo identificado?
4. ¿Qué diferencias existen entre una política, un estándar y un procedimiento?
5. ¿Cuáles son las responsabilidades de los dueños y custodios de datos?

CAPÍTULO 3

CONTINUIDAD DEL NEGOCIO

PARA APROVECHAR ESTE CAPÍTULO

» **LISTAR** LA INFORMACIÓN QUE ESTAMOS RESPALDANDO Y VERIFICAR SI ES LA CORRECTA, ASÍ COMO TAMBIÉN CONTROLAR LA FORMA EN QUE LO HACEMOS.

» **IMPLEMENTAR** ALGUNO DE LOS PROGRAMAS DE MONITOREO AQUÍ MENCIONADOS, AUNQUE SEA SOLAMENTE EN UN AMBIENTE DE PRUEBAS.

» **PENSAR** EN QUÉ FORMA RESPONDERÍAMOS ANTE UN EVENTO ADVERSO Y CUALES VERDADERAMENTE MERECE NUESTRA ATENCIÓN

CONTINUIDAD DEL NEGOCIO

En este capítulo aprenderemos a:

Objetivo 1 Seleccionar qué datos respaldar y de qué manera hacerlo.

Objetivo 2 Mantener el control de nuestra infraestructura a través del monitoreo.

Objetivo 3 Estar preparados para responder correctamente ante los eventos adversos.

Hasta ahora hemos analizado las tareas que debemos llevar a cabo para prevenir o minimizar las probabilidades de que nuestros sistemas sufran algún impacto negativo, analizando los riesgos y teniéndolos bajo control. Con estos cuidados, ya tenemos la mitad de la batalla ganada. ¿Cuál es la otra mitad? Saber qué debemos hacer cuando las cosas malas suceden.

Parte de ser excelentes profesionales recae en nuestra capacidad de estar al tanto de la completa situación de la infraestructura y poder conocer eventos futuros. Así estaremos completamente preparados y responderemos de la mejor manera posible.

A esto se lo conoce como "continuidad del negocio", e implica tener la capacidad de hacer resistente una organización: resistente a los eventos adversos y a aquellas situaciones que, de no estar preparados, la harían desaparecer. Esto no es poca cosa y, así como es difícil garantizar la subsistencia financiera de una empresa, es difícil garantizar la subsistencia de los sistemas. Pero ahí se encuentra gran parte

de la diversión de nuestro trabajo: en la incertidumbre y los riesgos a los cuales tenemos que hacer frente con frecuencia. Deberemos tener en cuenta una gran cantidad de variables para poder realizar un planeamiento correcto. Este es un proyecto largo y complejo, que nos consumirá un tiempo considerable; claro que, si lo hacemos bien, los resultados serán más que satisfactorios, y el nivel de seguridad de nuestra organización aumentará notablemente.

Las pérdidas siempre van a estar, al igual que los accidentes y los ataques. Queda en nosotros hacer el mejor esfuerzo para que este tipo de eventos nos afecte lo menos posible

En las siguientes páginas analizaremos cómo debemos realizar el planeamiento y la redacción de documentos correspondientes a la continuidad del negocio de nuestra organización. Cada uno de estos pasos nos será de vital importancia, tanto en los momentos de trabajo diario como en los de crisis, durante los cuales deberemos saber exactamente qué hacer y cómo lograrlo.

COPIAS DE RESPALDO

Dios se apiada de la persona responsable de mantener las copias de seguridad si estas no funcionan cuando se las necesita.

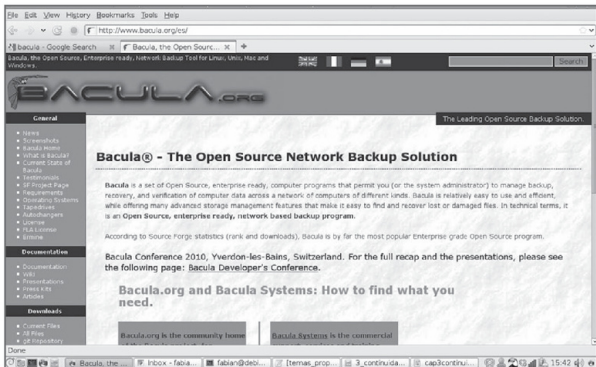
Una copia de seguridad es como contratar un seguro médico: esperamos nunca tener que usarlo, pero si lo necesitamos, tiene que responder a la perfección



Como no es habitual tener la necesidad de restaurar una copia de seguridad, las empresas suelen restarle importancia al proceso de realizarlas. Al ser encargados de la seguridad, esta es una de nuestras tareas: hacer que todos los datos de valor para la organización sean respaldados regularmente, y que estos respaldos sean probados en intervalos de tiempo determinados.

Principalmente, debemos basarnos en el testimonio de los dueños de datos a la hora de definir cada cuánto realizar los backups y por cuánto tiempo almacenarlos. Además, habrá que tener en cuenta las disposiciones legales y regulatorias, que muchas veces exigen determinados criterios de almacenamiento. Si no tenemos definidos los dueños de datos, tendremos que utilizar el resultado de la clasificación de activos. Y si no hicimos la clasificación de activos, podremos usar nuestra intuición, ¡o empezar a implementar lo que aprendimos en el **Capítulo 2!**

*Figura 1. Para obtener más información sobre **Bacula**, podemos entrar a su sitio web: www.bacula.org.*



El 90% de las empresas que sufren una pérdida de datos importante desaparece del mercado en dos años

(Fuente: Cámara de Comercio de Londres, www.londonchamber.co.uk)

Bacula es una herramienta para realizar copias de seguridad. Es de código abierto y multiplataforma. Funciona con la arquitectura cliente/servidor y nos permite instalar agentes en cada uno de los equipos que queremos respaldar, configurando varias opciones.

La selección del lugar en donde vamos a almacenar las copias de seguridad dependerá de qué eventos adversos esperamos que puedan suceder. Si queremos contemplar la posibilidad de un incendio o una inundación en nuestro centro de datos, no sería nada inteligente almacenar las copias en ese mismo sitio. Por lo general, suele ser suficiente elegir un lugar que esté en el mismo edificio, pero lejos del centro de datos, y protegido por una caja fuerte a prueba de calor.

Figura 2. BackupExec es un conjunto de productos para la generación de copias de respaldo, su gestión y la recuperación de datos. Además, nos permite recuperar sistemas enteros, ya sea Windows o Linux, sobre hardware tanto real como virtual (www.symantec.com).

RECOMENDADOS

Algunas de las herramientas de código abierto que pueden simplificar el proceso de realizar y mantener copias de seguridad son Bacula (www.bacula.org), Amanda (www.amanda.org) y BackupPC (<http://backuppc.sourceforge.net>). También existen otras propietarias, como Acronis (www.acronis.com), Arkeia (www.arkeia.com) y EMC Networker (www.emc.com).

En otros casos, nos encontraremos ante la necesidad de almacenarlos fuera del edificio, ya sea en un centro de datos alternativo o en alguna otra ubicación. Además, es necesario que verifiquemos periódicamente el funcionamiento de los métodos de recuperación. No hace falta probar cada una de las copias, pero sí tenemos que seleccionar una al azar para hacerlo. Eso nos dará la seguridad tanto de que los datos están ahí, como de que las herramientas empleadas funcionan correctamente.

Como siempre, el uso de herramientas automatizadas nos permitirá ahorrar horas de trabajo y evitar errores, por lo que es fundamental elegir una buena herramienta. Además, debemos tener



en cuenta no solo los tipos de datos que queremos resguardar, sino también los que podemos necesitar resguardar en un futuro, porque no todas las herramientas son compatibles con todos los datos o con todos los requerimientos particulares. Por ejemplo, existen algunas especialmente preparadas para realizar copias de seguridad de determinados tipos de software, como bases de datos, servidores de correo electrónico, y otros. También es una excelente idea seleccionar una herramienta que pueda ser

MUST KNOW

Es preciso tener en cuenta que las copias de seguridad deben ser cuidadas como un activo más de información. Suelen contener datos confidenciales, por lo que siempre es recomendable encriptarlas. Además, deben ser fácilmente identificables para que el encargado de restaurar los datos pierda el menor tiempo posible en buscar la copia correcta.

DEL EXPERTO

POLÍTICA DE BACKUP

Una de las decisiones importantes que debemos tomar al definir nuestra política de copias de seguridad es seleccionar los medios de almacenamiento que vamos a utilizar. Principalmente, podemos optar por discos ópticos (CD, DVD, Blu-ray, etc.), cintas magnéticas, discos de red (NAS) o dispositivos del tipo 'storage'. De todos ellos, los más recomendables son los discos de red o los dispositivos de storage para las copias locales y de grandes volúmenes de datos, y las cintas o medios ópticos para el transporte a locaciones remotas. En la imagen se muestran las principales ventajas y desventajas de cada uno. Debemos tener en cuenta factores como la capacidad de almacenamiento, el costo por Gigabyte, la velocidad de transferencia de información y la durabilidad del medio. Por último, debemos considerar el hardware que necesitamos para poder acceder a la información. Particularmente, las cintas magnéticas requieren de lectores especiales, que no se encuentran en todos los entornos de trabajo.

extendida para soportar nuevos tipos de datos, ya sea que tengamos que hacer el desarrollo nosotros mismos o debamos contratar un consultor especializado. Esto nos permitirá contar con la misma herramienta aunque la infraestructura y los requerimientos cambien.

Más allá de esto, si no podemos contar con la herramienta perfecta, por lo menos debemos disponer de copias de seguridad realizadas a mano, con la mayor responsabilidad posible. Con el tiempo, y en la medida en que podamos mejorar nuestros procesos, iremos adquiriendo las herramientas adecuadas para efectuar cada tarea, y así optimizar los tiempos y minimizar los errores.

El robo externo de datos corresponde al 24% de las causas de pérdidas y fugas de información

(Fuente: Symantec 2010 SMB Information Protection Survey)

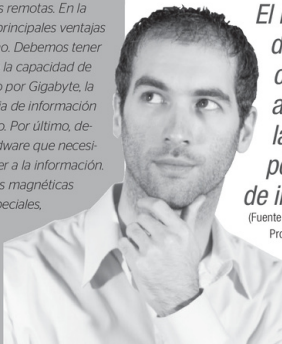
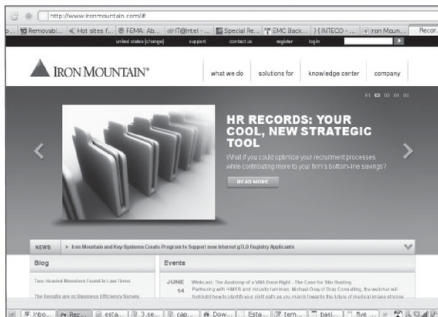


Figura 3.

IronMountain es una empresa especializada en la protección de datos y recuperación ante desastres. Publicó un interesante documento llamado "Las cinco mejores prácticas para proteger tus copias de seguridad" (www.ironmountain.com).

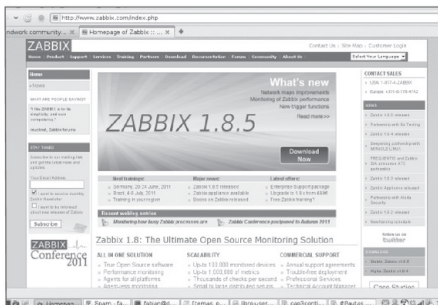


MONITOREO

Un aspecto que nos será de gran utilidad en nuestro trabajo cotidiano, y que nos servirá para impresionar a nuestros jefes, es la posibilidad de conocer rápidamente el estado completo de la infraestructura tecnológica. Esto nos permitirá mantener los problemas a raya, al poder controlar las cosas antes de que sucedan, y

asombrará a nuestros superiores, porque demostrará que tenemos el control de la situación, lo cual siempre es bueno. Existen varias formas de monitorear una infraestructura, pero la más recomendable es utilizar una herramienta especializada. Esto nos dará la gran ventaja de poder centralizar todo el monitoreo en un solo lugar, ya sea de plataformas Windows, Linux, aplicaciones, y cualquier otro parámetro que queramos

Figura 4. Zabbix es una excelente herramienta de monitoreo. Escrita en PHP, puede utilizar bases de datos tanto MySQL como PostgreSQL. Es de código abierto, así que podemos descargarla desde su sitio oficial y utilizarla libremente (www.zabbix.com).



RECOMENDADOS

Existen varias herramientas de código abierto destinadas al monitoreo de infraestructuras. Algunas cuentan con versiones comerciales que ofrecen una mayor cantidad de características y tienen soporte del fabricante. Por ejemplo: Pandora (<http://pandorafms.com>), Zabbix (www.zabbix.com), Hyperic (www.hyperic.com) y Zenoss (www.zenoss.com).

MUST KNOW

Aunque por diversos motivos no podamos implementar la solución de monitoreo que creamos ideal, es recomendable tener, por lo menos, "algo" que nos permita estar al tanto de la situación de nuestra infraestructura. No es necesario que sea un sistema avanzado; basta con que se nos envíe un correo electrónico si se detecta una situación anormal.

seguir de cerca. Como siempre, la selección de la herramienta queda en manos de cada profesional, según sus gustos y necesidades particulares. De esto, lo más importante es hacer la elección sobre la base de toda la estructura, teniendo en cuenta que, en algún momento u otro, necesitaremos monitorear cada uno de nuestros activos de información. Así que, al seleccionar dicha herramienta, será preciso tener presentes nuestras necesidades tanto actuales como futuras. Otra de las grandes ventajas que tiene el uso de una herramienta frente a alguna solución más simple, como los típicos scripts de monitoreo, es que en

ellas podremos definir varios usuarios, y perfiles para cada uno. Con esto, será posible asignar permisos de acceso a cada integrante de la organización, de acuerdo con lo que cada uno necesite. Esta es una ventaja que podemos perder de vista al principio, pero que, luego, se vuelve necesaria si precisamos dividir las tareas de gestión de la seguridad. Si bien algunas de las características de Nagios se han quedado en el tiempo, sigue siendo una opción

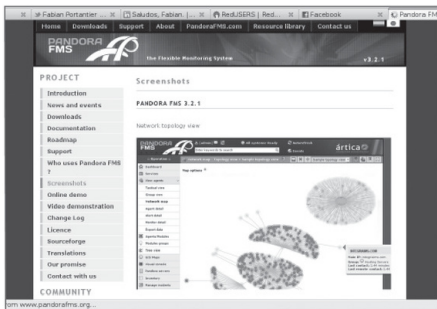
Figura 5. Nagios es una de las herramientas de código abierto más populares para el monitoreo de redes y servidores.

The screenshot shows the Nagios website homepage. At the top, there's a navigation bar with links: Network, Enterprise, Support, Library, Project, Exchange. Below this is the Nagios logo and the OpenGear logo. A secondary navigation bar contains links: Home, News, Products, Documentation, Support, Projects, About, Get Involved, Whats New, Download. The main content area has a heading "Welcome To Nagios - The Industry Standard in IT Infrastructure Monitoring" followed by a list of bullet points:

- Learn - Learn what Nagios is and what it can do for you.
- See - See screenshots of Nagios in action.
- Download - Get Nagios and start using it.
- Extend - Enhance your install with thousands of Nagios addons.
- Get Support - Get community and commercial support.
- Contribute - Find ways to get involved with Nagios.
- Whats New - Learn about the newest Nagios developments.

 To the right of the list is a "See Nagios Screenshots" link and a "Download Nagios" button. Below the download button is a "Support" section with the text "Get help with community and commercial support options. Learn More >". At the bottom, there's a "Featured Products" section listing "Websensor EN08F WiFi" and "Monitor temperature". The footer contains "Latest Nagios News" and "Community Blog" links.

Figura 6. La plataforma PandoraFMS es una excelente opción para monitorear servidores, equipos de telecomunicaciones y prácticamente cualquier otro dispositivo o servicio de red. Está desarrollada por la empresa española Artica (www.pandorafms.org).



muy potente. La versión paga se encuentra más actualizada y preparada para ofrecer características muy interesantes, además de tener soporte del fabricante (www.nagios.org).

El 73% de las empresas ha detectado ciberataques en su contra. De ellos, el 80% ha causado impacto negativo en su operatoria

(Fuente: Symantec 2010 SMB Information Protection Survey)

MUST KNOW

Los sistemas de detección y prevención de intrusos son un excelente recurso, tanto para monitorear nuestra infraestructura (detección) como para bloquear ataques en tiempo real (prevención). Si queremos tener nuestra infraestructura verdaderamente controlada, será preciso implementar sistemas de detección a nivel tanto de host como de red.

Si bien el monitoreo está relacionado directamente con las herramientas de monitoreo de red y servidores, y existen muchas tecnologías y protocolos para realizar estas tareas (como SNMP y WMI), el de seguridad abarca mucho más que eso. Este tipo de herramientas suele basar su funcionamiento en la disponibilidad de los servicios, mientras que, como ya vimos, la seguridad también debe considerar la confidencialidad y la integridad. Por lo tanto, necesitamos implementar herramientas complementarias o cualquier otra forma de obtener los datos que buscamos. Algunos de los parámetros que podemos necesitar seguir de cerca, y que se relacionan directamente con la confidencialidad y la integridad de los datos, son:

- » Modificación de archivos críticos.
- » Estado de encriptación de las telecomunicaciones.
- » Cantidad de ataques de malware.

Rápidamente podemos darnos cuenta de que estos valores tienen varias diferencias con los parámetros clásicos que se monitorean en una red. Y también observaremos que la obtención de estos valores se realizará por medio de varias fuentes de información, como el software

antivirus, los routers y los agentes que tengamos instalados en los servidores. Esto hace que tengamos que integrar varias herramientas, ya sea de forma manual o automatizada, lo que determina que el monitoreo completo de la seguridad informática sea una tarea compleja, que requiere de un planeamiento muy inteligente. Será cuestión de práctica y experiencia el hecho de ir perfeccionando nuestras capacidades de monitoreo y lograr la integración entre cada una de las herramientas que utilizemos. Con el correr del tiempo, sabremos puntualmente qué valores debemos seguir de cerca y cuáles no son tan importantes.

CONTROL DE CAMBIOS

Si hay una particularidad que destaca a la tecnología es que cambia constantemente, y esto nos lleva a tener que hacer grandes esfuerzos para mantenernos actualizados con lo último del mercado. Cuando estamos en la lucha por mantenernos actualizados, a veces perdemos el foco y olvidamos tomar los recaudos de seguridad

Una de las causas más comunes de las nuevas brechas de seguridad y de los desastres en los sistemas informáticos es la pérdida de control sobre los cambios que estos sufren

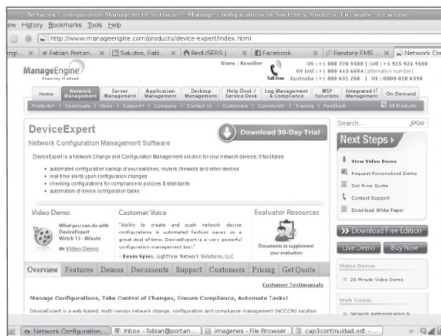


Figura 7. DeviceExpert es una plataforma para la gestión de configuraciones de dispositivos de red, desarrollada por la empresa Manage Engine (www.manageengine.com).

MUST KNOW

Al decidir si hacemos una actualización, debemos tomar en cuenta varios factores, como las nuevas funcionalidades, las mejoras en la seguridad, la estabilidad y la compatibilidad con otros componentes del sistema. No siempre decidiremos hacer las actualizaciones, pero lo más importante es que efectuemos un análisis antes de tomar la decisión.

necesarios. Muchas veces se utiliza el concepto de "siempre actualizar", como si cada uno de los sistemas debiera estar en su última versión para funcionar correctamente o cumplir con las políticas de seguridad. Esta es una verdad a medias, por dos motivos fundamentales. Primero, hay que evaluar si la última versión es considerada "estable", porque ciertos equipos de desarrollo suelen publicar versiones de software que son de prueba y que, si bien pueden tener pocos errores, aún no han sido testeadas como para instalarse en equipos de producción. Segundo, las actualizaciones no siempre traen mejoras de seguridad, y muchas veces, presentan más requerimientos de hardware o dependencias de software. Por lo tanto,

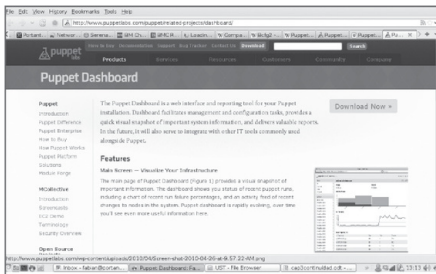
es preciso tener cuidado al decidir si aplicamos las actualizaciones o no.

Por otro lado, también tenemos los cambios de configuraciones, que suelen hacerse en equipos de producción, sin tener en cuenta que pueden provocar caídas del sistema, problemas de rendimiento y hasta pérdidas de datos. Para este tipo de situaciones, también podemos contar con herramientas que nos permitan mantener distintas versiones de las configuraciones del sistema. Lamentablemente, como cada sistema utiliza su propio método de configuración (bases de datos, archivos de texto plano, archivos XML, formatos propietarios, ldap, etc.), es muy difícil encontrar una única herramienta con la cual mantener todas nuestras configuraciones. En

RECOMENDADOS

Para la gestión de configuraciones, NAI es una excelente herramienta de código abierto que puede correr en plataformas tanto Windows como Linux y MAC (<http://inventory.alterpoint.com>). También podemos optar por las herramientas pagas como Orion, de Solarwinds (www.solarwinds.com); y DeviceExpert, de Manage Engine (www.manageengine.com).

Figura 8. Puppet es una herramienta para la gestión de configuraciones de sistemas de tipo UNIX. Está desarrollada en Ruby, cuenta con una gran comunidad de usuarios y dispone de varios recursos de documentación (www.puppetlabs.com).



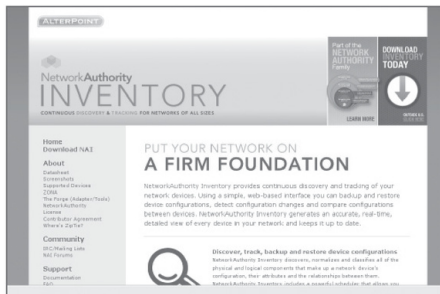


Figura 9. La herramienta de código abierto NAI (antes conocida como Ziptie) nos permitirá gestionar un inventario de nuestros activos de red, mantener versiones de archivos de configuración y realizar varios tipos de pruebas (<http://inventory.alterpoint.com>).

este caso, todo dependerá de nuestras necesidades, de nuestra creatividad y de nuestra capacidad para desarrollar herramientas propias, mezclándolas con las ya existentes. También debemos analizar los criterios para seleccionar los productos que vamos a implementar, teniendo en cuenta los métodos de configuración disponibles, a fin de simplificar el mantenimiento y la gestión de las configuraciones.

AMBIENTES DE PRUEBAS Y PRODUCCIÓN

Cuando nos encontramos frente a la situación de tener que implementar una modificación –ya sea por una actualización de software o hardware, o por un cambio de configuración–, sabemos

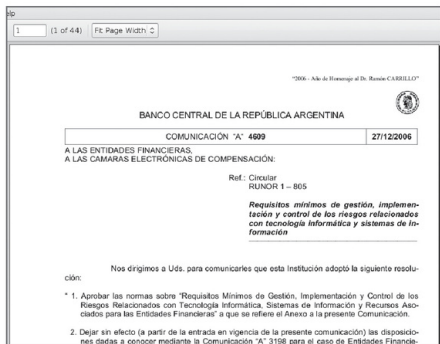


Figura 10. Algunas normativas, como la BCRA4609 –emitida por el Banco Central de la República Argentina–, exigen a sus entidades reguladas contar con ambientes separados de desarrollo, pruebas y producción. Otras normativas y estándares tienen exigencias similares (www.bcra.gov.ar).

que existe el riesgo de provocar una caída en el sistema o la pérdida de datos. Es por eso que se vuelve extremadamente recomendable contar con un ambiente de pruebas idéntico al de producción, que nos sirva para probar los cambios y verificar que todo funcione correctamente. De ser posible, debemos tener un sistema de pruebas por cada sistema de producción. Si no disponemos de los recursos necesarios, como mínimo necesitaremos sistemas de pruebas que se correspondan con los sistemas de producción más críticos. Para esto, podemos hacer uso de la virtualización, que nos permitirá crear equipos virtuales de pruebas en pocos minutos. Es importante entender que un equipo de pruebas no deja de ser un equipo de nuestra infra-

Figura 11. Mantis es una herramienta que nos permite mantener un registro de incidentes, hacer seguimientos y reportes, y muchas otras tareas más. Es bastante personalizable y, por si esto fuera poco, es de código abierto, está escrita en PHP y utiliza una base de datos MySQL.

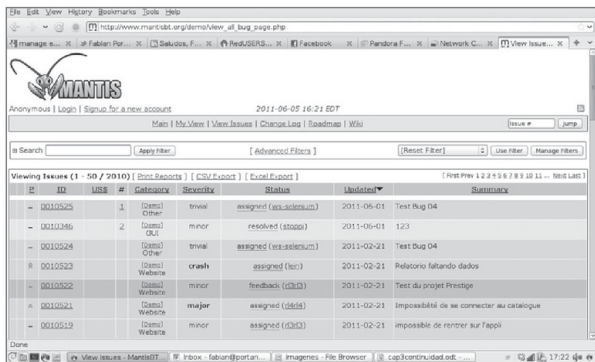
Cuando ocurre un incidente de seguridad, lo más importante es saber exactamente qué hacer

estructura, y debe ser protegido como tal. Para esto, tendremos que implementar las políticas de seguridad correspondientes y tratar de mantenerlo lo más aislado posible de los equipos de producción, de modo que no haya ningún tipo de inconveniente entre ellos.

Además, es necesario que cada equipo de pruebas tenga bien identificado su rol "de pruebas", y no sea utilizado para absolutamente ninguna tarea de producción.

GESTIÓN DE INCIDENTES

De acuerdo con la gravedad del asunto, tal vez tengamos que reaccionar de manera inmediata, con lo cual será de suma importancia tener a



The screenshot shows the Mantis Bug Tracker web interface. At the top, there's a navigation bar with links like 'Main', 'My View', 'View Issues', 'Change Log', 'Roadmap', and 'Wiki'. Below this is a search bar and a table of 'Viewing Issues (1 - 50 / 2010)'. The table has columns for ID, User, Category, Severity, Status, Updated, and Summary. The issues listed are:

ID	User	Category	Severity	Status	Updated	Summary
0010525	[demo]	Other	trivial	assigned (jes-selenium)	2011-06-01	Test Bug 04
0010346	[demo]	GUI	minor	resolved (stoppi)	2011-06-01	123
0010524	[demo]	Other	trivial	assigned (jes-selenium)	2011-02-21	Test Bug 04
0010523	[demo]	Website	crash	assigned (len)	2011-02-21	Relatorio faltando dados
0010522	[demo]	Website	minor	feedback (d3d3)	2011-02-21	Test du projet Prestige
0010521	[demo]	Website	major	assigned (d3d3)	2011-02-21	Impossibilité de se connecter au catalogue
0010519	[demo]	Website	minor	assigned (d3d3)	2011-02-21	impossible de rentrer sur l'apoi

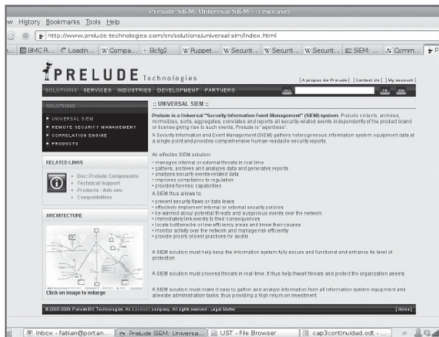


Figura 12. Prelude es un SIEM de código abierto bastante interesante, que puede obtener datos de diversas fuentes, como Snort, OSSEC y otras herramientas de detección de intrusos, así como de herramientas de monitoreo (www.prelude-technologies.com).

mano las herramientas y la información correctas. Es ampliamente recomendable contar con un sistema de seguimientos de incidentes, a fin de registrar cada uno de los problemas que van surgiendo, con sus respectivas soluciones. Esto nos dará la posibilidad de hacer un análisis estadístico de nuestros tiempos de respuesta y de los problemas más frecuentes.

Cerca del 20% de las empresas desconoce el número de incidentes de seguridad ocurridos en los últimos 12 meses

(Fuente: PWC Global State of Information Security Survey 2011)

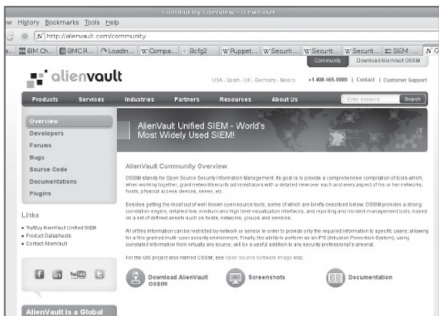


Figura 13. OSSIM es un SIEM desarrollado por la empresa AlienVault, que se basa en la agrupación de varias herramientas de código abierto, como Snort, Nagios, OpenVas y algunas otras. Cuenta con una versión paga que ofrece algunas capacidades extra, además del soporte del fabricante (<http://alienvault.com>).

Para definir la criticidad de un incidente, debemos basarnos en la clasificación de activos, analizando a cuáles afecta y qué problemas produce. Esto también nos permitirá saber de qué tenemos que ocuparnos primero si se presentan varios incidentes al mismo tiempo o hay varios activos afectados.

También existen herramientas que integran el monitoreo con la prevención de intrusos, el seguimiento de incidentes y otras funciones de seguridad. Se las denomina SIEM (*Security Information and Event Management*).

Las herramientas del tipo SIEM suelen ser complejas, y puede llevar un tiempo configurarlas correctamente y acostumbrarnos a utilizarlas.

Pero, una vez que dominemos su uso, pueden ahorrarnos muchísimo tiempo y brindarnos la capacidad de centralizar una gran cantidad de tareas en un mismo lugar.

Además, suelen estar preparadas para conectarse con herramientas externas, lo que las convierte en un excelente recurso para la gestión de grandes infraestructuras, que cuentan con una

variedad de sistemas que obliga a los administradores a utilizar varias herramientas diferentes.

Es una excelente idea probar este tipo de sistemas, utilizarlos durante un tiempo y ver con cuáles nos sentimos cómodos, analizando qué beneficios podemos tener a corto y largo plazo.

Las caídas de servicio representan el 49% de los impactos que ocurren en una organización tras un ataque

(Fuente: Symantec 2010 SMB Information Protection Survey)

Los SIEM pagos suelen tener precios elevados, así que tendremos que pensarlo bien antes de tomar una decisión. Todo dependerá de la cantidad de recursos con los que contemos para llevar a cabo la gestión de la seguridad. Si disponemos de buenos recursos económicos pero estamos acotados en cuanto a recursos humanos, la instalación de un SIEM puede

Figura 14. El Foro de Equipos de Respuesta a Incidentes de Seguridad (FIRST) es una entidad que organiza a varios de los equipos de respuesta a incidentes (CERT) del mundo. Allí podemos encontrar diversos recursos de interés (www.first.org).

The screenshot shows the website of the Forum of Incident Response and Security Teams (FIRST). The header includes the FIRST logo and the text "Forum of Incident Response and Security Teams". Below this, there is a banner for the "23rd Annual FIRST Conference" in Vienna, Austria, from June 12-17, 2011. The banner includes a "Register now" button and a "Search | Site Map" link. Below the banner, there is a section titled "FIRST is the global Forum for Incident Response and Security Teams". This section describes FIRST as the premier organization and recognized global leader in incident response, and lists sponsors for the upcoming conference, including S21 sec CERT (Spain), IRIS-CERT and INTECO-CERT (NTDRA-CERT) (Lisbon), NTT-CERT and JPCERT/CC, and CERT-PT (Portugal).



Figura 15. Aunque la organización DRI Internacional no se enfoca directamente en la seguridad informática, es un excelente recurso de información; su sitio es www.drill.org.

“Un punto clave al responder ante una emergencia es la frialdad con la que lo hacemos, porque la presión puede hacernos actuar equivocadamente

optimizar todas nuestras tareas, lo cual puede terminar siendo un ahorro de dinero para la organización. Además, este tipo de herramientas suele dar la posibilidad de generar reportes, los cuales nos servirán para los procesos de análisis y mejora

EN LA PRÁCTICA PROFESIONAL

Tomando como ejemplo un evento catastrófico, los ataques terroristas del 11 de septiembre de 2001 al World Trade no solo implicaron una pérdida enorme de vidas, sino que también destruyeron negocios por completo y dejaron a muchas empresas al borde de la quiebra. Muchas de ellas contaban con todos sus recursos apostados en un mismo lugar, tanto los humanos como los tecnológicos, y por eso no pudieron resistir la catástrofe. Esto nos demuestra que la cantidad de eventos adversos que podrían llegar a ocurrirnos es infinita, y no podemos estar preparados para cada uno de ellos. Pero sí es necesario que estemos al tanto de las situaciones más probables con las que podríamos llegar a tener que lidiar. Sobre la base de estos análisis, podremos seleccionar qué medidas de seguridad implementar, y tener una idea clara de los riesgos que están cubiertos y los que no lo están. Siempre es preferible saber que hay riesgos para los cuales no nos estamos preparando, que desconocerlos en su totalidad.



continua. Debemos tener en cuenta que, más allá de las herramientas que podamos utilizar, la gestión de incidentes no deja de ser otra cosa que estar al tanto de todo lo que sucede en nuestra infraestructura y enterarnos, de una forma u otra, de todo lo que suceda con la mayor rapidez posible. Una vez detectados, los incidentes deben resolverse en tiempo y forma. En resumen, la gestión de incidentes es el conjunto de políticas, metodologías, herramientas y procedimientos que se llevan a cabo para lidiar con todos los eventos adversos que sucedan en nuestros sistemas.

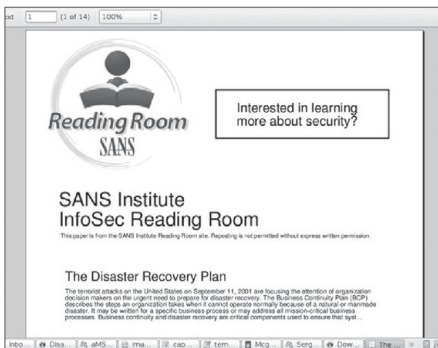
BIA, BCP Y DRP

Cuando nos ponemos a pensar en todas las cosas malas que pueden ocurrirles a nuestros sistemas, solamente hay una que puede mantenernos tranquilos: tener un plan. Y, si bien es cierto que no podemos estar preparados para responder ante absolutamente todas las cosas que pueden suceder, el hecho de saber que estamos preparados para afrontar las situacio-

“Si el documento BIA sirve para identificar qué es lo peor que puede pasarnos, los BCP y DRP sirven para saber qué hacer si esto nos pasa

nes adversas más probables no solo nos da seguridad, sino que también nos obliga a conocernos mejor. Es por eso que muchas veces, al tratar de reparar un desastre, producimos otro mucho mayor. Por lo tanto, en las situaciones de

Figura 16. El instituto SANS ha publicado un documento de trece páginas acerca de la recuperación ante desastres en sistemas informáticos. Es una excelente fuente de información, junto con las otras publicaciones de dicho instituto (www.sans.org).



MUST KNOW

Como los documentos BCP y DRP cumplen funciones bastante similares, podemos darnos el lujo de unificar el contenido de ambos en uno solo, siempre y cuando nuestra organización lo amerite. Por lo general, pueden unificarse en pequeñas y medianas empresas, y deben estar separados en grandes organizaciones, que tienen una estructura más compleja.

estrés que no nos permiten pensar es necesario tener un plan que lo haga por nosotros.

La **organización DRI International** se encarga de promover las actividades de continuidad de negocio y recuperación de desastres a través de educación, asistencia y publicación de documentación relevante.

Las siglas BIA, BCP y DRP hacen referencia a **Business Impact Analysis, Business Continuity Plan y Disaster Recovery Plan**, respectivamente.

El BIA (o análisis de impacto en el negocio) es el estudio que indica cuáles serían las situaciones

que tendrían un impacto más negativo en la operatoria de una organización. Suele ser un estudio que no considera solamente la tecnología, sino que abarca todas las posibilidades, como desastres naturales, problemas de imagen, muerte de personal de puestos críticos, cambios en la economía local y global, etc.

El proceso de desarrollo de este tipo de documentos es complejo, y abarca cuestiones que van mucho más allá de la seguridad informática, así que no vamos a detenernos mucho en este tema. Pero a continuación mostramos un listado de los pasos clave para poder crear un documento de estas características:

1. El primero es seleccionar a los individuos que vamos a consultar para esto.
2. Elegir las técnicas para obtener datos (cuestionarios, entrevistas, etc.).
3. Identificar las funciones críticas del negocio.
4. El cuarto paso es identificar los recursos que son necesarios por estas funciones.
5. Calcular durante cuánto tiempo pueden sobrevivir estas funciones sin esos recursos.
6. Identificar las vulnerabilidades y amenazas para estos recursos.



Figura 17. En el sitio del Business Continuity Institute podemos encontrar varios recursos acerca de las mejores prácticas para la continuidad del negocio, además de referencias a cómo obtener la certificación BCI (www.thebci.org).

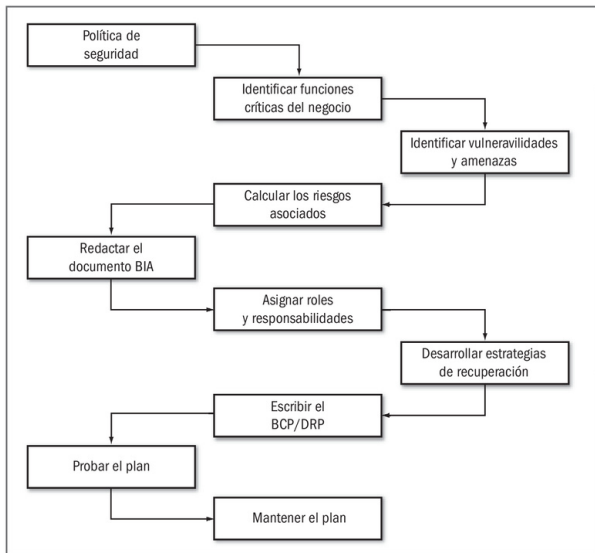


Figura 18. El gráfico muestra los principales pasos que deben llevarse a cabo en el desarrollo y mantenimiento de un BCP/DRP. Es un proceso complejo, y cada uno de los puntos mencionados lleva tiempo y tiene varias tareas asociadas.

7. Calcular el riesgo asociado a cada función del negocio.
8. Documentar los datos encontrados y reportarlos a la gerencia.

Como podemos observar, el proceso de desarrollo del BIA es muy similar a lo que vimos en el análisis de riesgos. La particularidad que tiene es que debemos considerar cualquier tipo de amenaza, no solo las relacionadas directamente con la información y la tecnología. Es por eso que, si nuestra organización no

dispone de un BIA, podemos utilizar el análisis de riesgos que se realizó en el **Capítulo 2** para llevar adelante los documentos BCP y DRP. La diferencia entre ellos es que el DRP se encarga de definir cuáles son las acciones que debemos tomar si sucede un desastre, mientras que el BCP se ocupa de definir cómo el negocio continuará funcionando mientras nos recuperamos de los efectos de ese desastre. Para simplificar nuestro trabajo, analizaremos el caso de una unificación de estos dos documentos, que resulta en un único BCP/

DRP. Para las organizaciones que lo requieran, que en la práctica son verdaderamente pocas, será necesario hacer un estudio minucioso y elaborar todo un proyecto para definir tanto un BIA, como un BCP y un DRP.

Pensando en una organización pequeña o mediana (y hasta en una organización grande, pero que tenga una estructura simple), nosotros vamos a trabajar sobre los datos obtenidos en el **Capítulo 2** (para evitar el desarrollo de un BIA) y a unificar la continuidad de nuestro negocio a través de un único documento BCP/DRP. Podemos decir que los puntos clave para el desarrollo del documento BCP/DRP son los siguientes:

1. Definir el proyecto para desarrollar el BCP/DRP. Asignar los roles, responsabilidades y autoridades de cada uno de los involucrados en el proceso. De este paso depende gran parte del orden con el cual se desarrollará el proyecto.
2. Sobre la base del análisis de riesgos, identificar las amenazas y vulnerabilidades que podrían llegar a desencadenar un desastre. Esto nos va

a servir para encaminar el proyecto y asignar prioridades a nuestras acciones.

3. Desarrollar estrategias de recuperación para cada una de las situaciones identificadas, tratando de unificar las medidas de recuperación, para reducir costos y simplificar el plan.

4. Escribir el plan de contingencia, con sus respectivos procedimientos y la asignación de roles para cada uno de los integrantes que deben intervenir en el proceso. Además, hay que explicar detalladamente cómo seguirá funcionando la organización mientras se recupera del desastre.

5. Probar el plan, realizar ejercicios de entrenamiento y capacitaciones. Esto es de vital importancia para asegurar que el plan funciona correctamente, y tener a los empleados bien preparados para responder en tiempo y forma.

6. Mantener el plan, tanto con actualizaciones periódicas, como buscando las formas de optimizar el documento, los procedimientos y a las personas involucradas. Si no hacemos esto, al cabo de poco tiempo, el plan quedará desactualizado y no nos servirá de nada.

	Ventajas	Desventajas
Cold Site	· Es el más económico	· Tarda mucho tiempo en volverse productivo. · Tenemos que llevar todo el equipamiento informático.
Warm Site	· Relación costo/beneficio. · Pueden probarse con relativa facilidad.	· Tenemos que llevar ciertos equipos informáticos.
Hot Site	· Disponible inmediatamente. · Las pruebas son fáciles de realizar.	· Costo muy elevado.

Figura 19. La tabla muestra, a grandes rasgos, las ventajas y desventajas de cada uno de los tipos de sitio de contingencia. Nuestra elección dependerá tanto del análisis de estos factores, como de nuestras necesidades y recursos disponibles.

SITIOS DE CONTINGENCIA

Ya sea porque una normativa nos lo pide o porque hemos evaluado que es necesario, puede ser necesario contar con un sitio de contingencia, que sirva para alojar sistemas de respaldo en caso de que los sistemas principales sufran daños. Este tipo de medidas es muy recomendable si queremos asegurar que podremos continuar con la operativa de la organización en situaciones catastróficas. La decisión de invertir en un sitio de contingencia debe salir del análisis de riesgos o del análisis de impacto en el negocio (BIA). Una vez que reconocemos la necesidad de un sitio de contingencia, nos queda seleccionar el tipo de sitio y el lugar en el que se encontrará. Los siguientes son los tres tipos de sitios entre los que deberemos elegir:

SITIO DE CONTINGENCIA EN FRÍO (COLD SITE)

Este tipo de sitios contiene la estructura básica, con electricidad, cableado y aire acondicionado, pero solamente eso; no incluye ningún equipamiento informático. Es la opción más económica, pero toma más tiempo en volverse operativa, porque tendremos que conseguir el equipamiento en el momento del desastre y configurarlo adecuadamente.

SITIO DE CONTINGENCIA TIBIO (WARM SITE)

Este tipo de sitios, además de contener lo mismo que uno frío, cuenta con algunos dispositivos informáticos, generalmente genéricos, como servidores, estaciones de trabajo y equipamiento de redes. Tarda menos tiempo en volverse operativo que un sitio frío, pero aun así, deberemos configurar los equipos y tal vez tengamos que conseguir el hardware que no es provisto por él. En algunas organizaciones que utilizan mainframes, servidores especiales o equipos de telecomunicaciones avanzados, podríamos tener que llevarlos y configurarlos.

SITIO DE CONTINGENCIA CALIENTE (HOT SITE)

Este tipo de sitios está completamente equipado y puede ponerse en marcha en pocas horas. Lo único que suele faltar en estos casos son los datos. El equipamiento instalado en ellos debe ser completamente compatible con el del sitio original. Obviamente, es la opción más costosa, sobre todo, si necesitamos que haya hardware muy particular o muy potente, pero nos garantiza la transición menos agresiva de un sitio a otro. Para la selección del tipo de sitio adecuado tendremos que analizar qué tiempos de caída de servicio podemos tolerar, las probabilidades de que ocurra un desastre y los recursos económicos de los que disponemos. La opción más utilizada son los sitios tibios, que suelen permitir un buen balance entre tiempos de respuesta y costo. En el caso de las organizaciones que no puedan soportar ni siquiera un día de pérdida de servicio, será necesaria la contratación de un sitio caliente. De todos modos, cualquiera de las opciones elegidas debe ser verificada periódicamente, para corroborar que los procesos de recuperación y el equipamiento del sitio funcionan como corresponde. Además, estas pruebas nos darán una buena idea de cuáles son nuestros tiempos de recuperación.

PARA PONER A PRUEBA

1. ¿Sobre la base de qué criterios debemos seleccionar los datos por respaldar y la frecuencia entre respaldos?
2. ¿Qué diferencia existe entre el monitoreo convencional de infraestructuras tecnológicas y el monitoreo de seguridad?
3. ¿Por qué se vuelve difícil unificar la gestión de las configuraciones de los distintos componentes de una infraestructura?
4. ¿Por qué es importante saber de antemano cómo reaccionar ante un evento adverso?
5. ¿Cuáles son las características de los distintos tipos de sitios de contingencia?

CAPÍTULO 4

TELECOMUNICACIONES

FACTOR CLAVE

PARA APROVECHAR ESTE CAPÍTULO

- » **ACCEDER** A LOS SITIOS RECOMENDADOS PARA APRENDER MÁS ACERCA DE LOS PROTOCOLOS.
- » **DESCARGAR** Y PROBAR EL SOFTWARE MENCIONADO.
- » **RELEVAR** LA DOCUMENTACIÓN DE TODOS LOS DISPOSITIVOS Y VERIFICAR QUÉ MEDIDAS DE SEGURIDAD PODEMOS IMPLEMENTAR.

TELECOMUNICACIONES

FACTOR CLAVE

En este capítulo aprenderemos a:

Objetivo 1 Comprender la importancia de los distintos tipos de dispositivos de telecomunicaciones.

Objetivo 2 Evaluar las ventajas y desventajas de implementar firewalls y sistemas IDS.

Objetivo 3 Seleccionar la mejor forma de administrar nuestros dispositivos.

Las **redes de computadoras** ya no son cosa del futuro, sino que están establecidas como algo común y corriente, casi implícitas en toda organización. Son un recurso tan habitual como el papel, y las empresas las utilizan para transportar datos a velocidades que, hasta hace unos años, eran imposibles de imaginar, como las redes inalámbricas. Todas estas tecnologías simplifican la vida de cada uno de los integrantes de una organización.

“Al plantear las estrategias de seguridad, la mayoría de las empresas tienden a enfocarse en

las estaciones de trabajo y los servidores,

porque estos son los equipos que almacenan y procesan la información con la que se trabaja día a día. Así que es común olvidar los dispositivos, las tecnologías y los protocolos que llevan esa información de un lugar a otro. Esto hace que, muchas veces, existan graves vulnerabilidades de seguridad, que no son detectadas hasta que algo malo sucede. Es por eso que cobra tanta importancia la visión global de la seguridad informática, que nos permite proteger una organización como un todo, y nos da la posibilidad de utilizar cada uno de nuestros dispositivos como una herramienta más de seguridad, en vez de verlos como puntos de falla. Recordemos que todo pasa por estos equipos, de modo que no podemos darnos el lujo de perder la oportunidad de controlarlos por completo, para sacar el máximo provecho de ellos.

Como expertos en seguridad, debemos tener una comprensión clara de las tareas que cumple cada uno de los dispositivos, así como también de los beneficios y las vulnerabilidades que pueden introducir en nuestra infraestructura. Es imposible evitar el uso de estos equipos, así que tendremos que aprender a seleccionarlos, configurarlos y mantenerlos de la manera adecuada. Es por eso que debemos tener en claro,

exactamente, cuáles son las herramientas y los recursos que tenemos a mano para prevenir y dar respuesta a los inconvenientes que surjan en esta área de la seguridad. En las siguientes páginas analizaremos en qué forma debemos proteger nuestras redes y qué herramientas podemos utilizar para simplificar nuestras tareas.

INVENTARIO DE DISPOSITIVOS

Como analizamos anteriormente, contar con un inventario de los dispositivos que se encuentran en una red es de vital importancia para poder implementar correctamente las medidas de seguridad adecuadas.

Para este tipo de tareas existen varias herramientas, muchas de ellas, de código abierto, como **Wireshark**, **Arpwatch**, **Ettercap**, y otras. Podemos ejecutarlas constantemente, y automatizarlas para obtener un reporte continuo de los nuevos dispositivos que aparecen en nuestra red. A continuación, analizaremos algunas distintas formas de llevar a cabo esta tarea.

40% de las empresas utiliza una solución de inventario de activos

(KPMG Information Security Survey)

SWITCHES INTELIGENTES

En caso de contar con **switches inteligentes**, podemos utilizar tecnologías como **Port Security** (presente en los dispositivos **Cisco**), que permite enviar una notificación a través de un **Trap SNMP** acerca de las nuevas **MAC** aparecidas en un puerto. Analizaremos **Port Security** con más detalle en uno de los siguientes apartados.

ARPALERT

Esta herramienta nos permite capturar el tráfico de una interfaz de red, y detectar las asociaciones de **IP** y **MAC actuales**, notificándonos de nuevos dispositivos y otro tipo de cambios. Es una herramienta de código abierto muy útil, que puede servirnos para crear rápidamente el inventario de una red.

Trabaja analizando los paquetes del tipo **ARP**, que se envían normalmente en una red para conocer la dirección **MAC** asociada a una **IP**. Como estos paquetes se mandan a todos los hosts de la red, podemos verlos y detectar de forma sencilla cuáles son los dispositivos activos.

SCRIPTING

Por último, podemos implementar una solución personalizada, automatizando herramientas como **Arpalert** o creando otras propias, a través de librerías como **Scapy**, para el lenguaje de

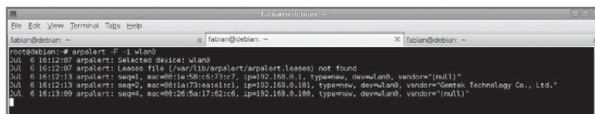


Figura 1. **Arpalert** es un software que nos alerta de cambios entre las asignaciones **MAC/IP**, lo cual puede ser muy útil como complemento de otras herramientas de monitoreo. En la imagen, podemos ver cómo nos alerta sobre la aparición de equipos nuevos en nuestra red. De ser posible, también nos detalla cuál es el fabricante asociado a la dirección **MAC** del equipo. (www.arpalert.org/arpalert.html)

programación Python. Este tipo de pequeños programas pueden ser de gran utilidad, por que nos permiten realizar tareas sencillas, y formular reportes, enviar correos electrónicos con notificaciones, y cualquier otra cosa que podamos precisar. Es necesario tener ciertos conocimientos sobre programación para desarrollarlos nosotros mismos, aunque podemos encontrar en Internet varios ejemplos y scripts completos, listos para utilizar. Para demostrar la potencia de Scapy, abajo tenemos un script que nos alerta de todas las consultas ARP que se realizan en una red. Con algunas pequeñas modificaciones, podríamos obtener un programa similar a arpalert, contenido en solo algunas líneas de código Arpalert.

```
#!/usr/bin/env python
from scapy.all import *

def arpmon(pkt):
    if ARP in pkt and pkt[ARP].op in (1,2):
        return pkt.sprintf("%ARP.hwsrc% %ARP.psrc%")

sniff(prn=arpmon, filter="arp", store=0)
```

Figura 2. Scapy
es una librería para el lenguaje de programación Python, que simplifica la tarea de crear paquetes de red personalizados. Con ella también podemos desarrollar rápidamente capturadores de tráfico y otras herramientas muy potentes (www.secdev.org/projects/scapy/).

ROUTERS Y SWITCHES

Si bien existen varios tipos de dispositivos de telecomunicaciones, los routers y los switches son, sin dudas, los más utilizados en la mayoría de las empresas. Tanto en equipos de gama alta como en los de gama baja, debemos considerar ciertos aspectos de seguridad al seleccionarlos, instalarlos y configurarlos, para sacar el máximo provecho a sus funcionalidades y proteger nuestros datos de la manera más adecuada.

Los switches son un caso especial, aún más olvidado, en general, porque hasta hace unos años los dispositivos que trabajaban en la

MUST KNOW

Aprender a programar scripts es de vital importancia para convertirnos en excelentes profesionales. Seguramente, pasaremos por diversas situaciones en las cuales este tipo de conocimientos puede simplificarlos en gran medida nuestras tareas. Y no es algo difícil de aprender: es cuestión de elegir un lenguaje y practicar. Para comenzar, es recomendable trabajar con Python.





Figura 3. Cisco Systems (www.cisco.com) es uno de los fabricantes de equipos de telecomunicaciones más reconocidos. Además del soporte brindado por la empresa, cuenta con una gran cantidad de recursos generados por la comunidad de usuarios.

EN LA PRÁCTICA PROFESIONAL

De ser posible, el inventario de activos debe obtenerse de la salida de varias herramientas, porque para realizarlo de forma adecuada es necesario obtener información de varias fuentes. Es una excelente práctica utilizar una herramienta central, que nos permita obtener un reporte general de los activos. La herramienta OCS Inventory permite tanto mantener un repositorio central de dispositivos, como implementar monitoreos constantes para detectar cambios y nuevos dispositivos de red. En los entornos de red pequeños, es posible utilizar una única fuente de información. Pero, en entornos de red grandes o muy segmentados, es recomendable utilizar varios sensores que nos permitan obtener datos de los diferentes puntos de la red. En el caso de las pequeñas empresas, que ni siquiera puedan contar con un entorno de servidor dedicado a esto, podemos implementar comprobaciones con comandos básicos, como 'ping', 'arping' y 'arpwatch', generando reportes en archivos de texto y alertas a través de correos electrónicos.



capa 2 del modelo OSI no eran gestionables ni configurables. Eso hizo que se los considerara como una especie de adaptador básico, que permitía unir varios dispositivos, así como lo hace el adaptador eléctrico, que nos permite conectar la televisión, la radio y el reproductor de DVD en un mismo enchufe. Esto ha cambiado, y tenemos que ponernos al corriente:

“los switches son cada vez más inteligentes e importantes para una red

Como primera medida, y como hemos visto en capítulos anteriores, debemos mantener un inventario de cada uno de nuestros dispositivos de comunicaciones. Para hacerlo, podemos recurrir a varios protocolos, de los cuales el más estandarizado y presente en todos los dispositivos del mercado es SNMP (**Simple**

Network Management Protocol). Algunos fabricantes tienen sus propios protocolos, como es el caso de Cisco con CDP. Sea cual sea el protocolo o la herramienta que utilicemos, es importante tener un inventario y estar al tanto del estado de cada uno de los equipos que componen la red.

Debemos ser cuidadosos con respecto a los puertos y servicios que habilitamos en nuestros dispositivos, y tratar de que sea la menor cantidad posible, además de configurar ade-

LA VISIÓN DEL EXPERTO

Cuando nos encontremos con la tarea de tener que seleccionar una solución de telecomunicaciones, debemos tener varios factores en cuenta antes de tomar una decisión, tanto de los equipos como de las tecnologías que vamos a utilizar. Una cuestión muy importante para considerar es el soporte que tendremos en caso de que se presente un problema o tengamos alguna inquietud. En este sentido, debemos considerar los planes de soporte que podemos contratar, tanto del fabricante, como de partners o consultores especializados. Para esto es fundamental tener en cuenta cuáles son los niveles de urgencia que podrían llegar a presentarse y la cantidad de recursos económicos de que podemos disponer. Si nuestras necesidades son grandes, podríamos optar por contratar a un nuevo empleado que se especializara en dicha solución, siempre analizando los costos y beneficios de esta alternativa. También debemos considerar como factor de importancia la documentación existente, tanto la oficial, como la que se encuentra foros, sitios web y otras publicaciones independientes.



MUST KNOW

No es necesario tener conocimientos avanzados sobre configuración de dispositivos de red, porque este es un tema bastante complejo. Pero es estrictamente imprescindible tener buenos conocimientos acerca de los protocolos más utilizados, como TCP/IP, y de los posibles problemas de seguridad que pueden presentar, así como de sus soluciones.

cuadamente las interfaces de administración para asegurarlas como corresponde.

PORT SECURITY

Esta es una tecnología que se encuentra disponible en varios modelos de switches. Algunos permiten realizar configuraciones más personalizadas que otros, pero la mayoría ofrece lo siguiente:

- » Lista blanca de MAC: permite definir qué dirección/es MAC pueden conectarse a qué puerto físico del switch. Es verdad que los usuarios avanzados podrán modificar su propia dirección MAC, pero esta es una medida de seguridad adicional muy útil.
- » Lista negra de MAC: permite definir qué dirección/es no podrán conectarse nunca a la red.
- » Aprender MAC: es posible definir que solamente las direcciones MAC conectadas en un momento puedan establecer conexiones, en tanto que los nuevos dispositivos estarán bloqueados.
- » Configuración remota: bloquea los dispositivos que pueden administrar el equipo en forma remota.

El siguiente ejemplo de configuración para un switch Cisco nos permite configurar Port Security en un determinado puerto, definiendo la dirección MAC permitida y la acción que se tomará en caso de que se detecte una violación: deshabilitar el puerto (**shutdown**):



Figura 4. Juniper Networks es otro reconocido fabricante de equipos de telecomunicaciones. La empresa desarrolla su propio sistema operativo de red (JunOS) y cuenta con equipos de grandes prestaciones (www.juniper.net).

```
switchport port-security
switchport port-security mac-address
DIRECCION_MAC
switchport port-security violation shut
down
```

Port Security también impide que pueda realizarse un ataque de CAM-Overflow, en el cual la memoria CAM del switch se llena, y este empieza a trabajar como si fuera un hub, enviando todo el tráfico a todas las interfaces. Esto permitiría que un atacante viera información confidencial.



Figura 5. Este famoso sitio mantiene una lista con un ranking de las 100 mejores herramientas de seguridad para redes. Resulta de mucha utilidad como referencia. Actualmente, la lista es encabezada por Nessus, Wireshark y Snort. Nmap no se ha incluido, debido a que está desarrollando un recurso por las mismas personas que realizaron la lista. (<http://sectools.org>)

Siempre debemos analizar cuidadosamente la documentación de los dispositivos con los que contamos, para estar al tanto de las tecnologías que soportan, e implementarlas si consideramos que nos resulta conveniente

DHCP SNOOPING

Esta tecnología permite a los switches analizar los mensajes DHCP, y aprender las asociaciones entre direcciones IP y MAC. La idea principal es que el switch permita tráfico DHCP solamente con servidores DHCP autorizados. Este tipo de tecnología marca la nueva tendencia de los switches inteligentes, según la cual el dispositivo no solamente se limita a retransmitir pa-

EN LA PRÁCTICA PROFESIONAL

En Internet hay disponible una gran cantidad de documentos con mejores prácticas de seguridad. Debemos ser cuidadosos acerca de las fuentes de información que utilizamos y verificar que las configuraciones funcionen bien en un ambiente de pruebas antes de llevarlas a un ambiente productivo. Algunos de los documentos mejor redactados y más confiables son los desarrollados por la **National Security Agency** (NSA, (www.nsa.gov)). Entre otros, se han publicado guías de configuración para routers y switches Cisco, varios sistemas operativos y aplicaciones.

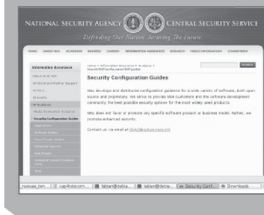
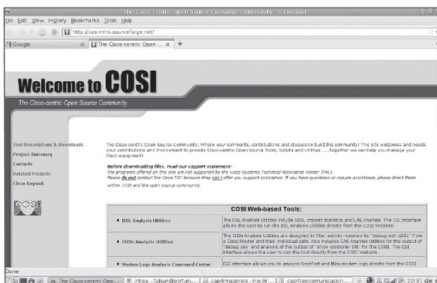


Figura 6. El sitio web COSI es un excelente lugar en el que se pueden encontrar varias herramientas de código abierto para trabajar con equipamiento Cisco, además de algunos otros recursos relacionados con la marca (<http://cosi-nms.sourceforge.net>).



quetes, sino que también se encarga de analizar el tráfico y bloquear los ataques más comunes. El DHCP Snooping también bloquea los ataques del tipo DHCP Starvation, en los cuales un atacante envía muchísimas peticiones DHCP con el objetivo de agotar todas las direcciones IP disponibles en el servidor.

CUENTAS DE ACCESO CENTRALIZADAS

Quando tenemos que administrar varios dispositivos, es una excelente idea centralizar nuestra base de datos de usuarios,

para poder asignar perfiles y simplificar nuestra tarea de altas, bajas y modificaciones.

La siguiente configuración nos permite definir un servidor TACACS+ para autenticar a nuestros usuarios en un router Cisco:

```
aaa new-model
aaa authentication login default tacacs
local
aaa authentication login consoleport
none
aaa authorization network tacacs
tacacs-server host 10.6.101.101
tacacs-server key cisco
```

Esto nos será de utilidad no solo para nuestros dispositivos de telecomunicaciones, sino también para todos nuestros servidores y otros equipos que requieran ser gestionados, y para los cuales podemos elegir entre varias tecnologías de control de acceso. Detallamos algunas de ellas a continuación.

MUST KNOW

Es de suma importancia que unifiquemos los usuarios y perfiles de acceso en una misma base de datos, tanto para los dispositivos de telecomunicaciones, como para los sistemas operativos. Esto reduce la posibilidad de cometer errores, y nos permite enfocar nuestros esfuerzos en un único lugar, lo que simplifica el trabajo de manera notable.

TACACS+

Es un protocolo desarrollado por Cisco, que nos provee de autenticación, autorización y registros (en inglés, las siglas AAA). Utiliza el protocolo TCP para el intercambio de datos. El tráfico es encriptado para brindar mayor seguridad a las comunicaciones entre los clientes y el servidor.

Podemos encontrar un servidor de TACACS+ de código abierto en www.shrubby.net/tac_plus.

RADIUS

A diferencia de **TACACS+**, **Radius** utiliza el protocolo UDP para el intercambio de datos, y unifica los procesos de autenticación y autorización, lo cual presenta dos desventajas. Pero sigue siendo una buena alternativa. Podemos encontrar un servidor Radius de código abierto en <http://freeradius.org>. Además, Microsoft Active Directory puede ser configurado para brindar servicios de Radius utilizando su base de datos de usuarios.

DIAMETER

Este protocolo es el sucesor de Radius, y cuenta con grandes ventajas, tanto sobre su predecesor como sobre TACACS+. Está encriptado con TLS, permite notificar errores, soporta servicios con roaming y es extensible para poder agregarle nuevas funcionalidades. Podemos encontrar un servidor Diameter de código abierto en www.freedomiameter.net.

UTILIZACIÓN DE SERVIDORES SYSLOG

Una de las formas de contar con un registro de todo lo que sucede en nuestros equipos de telecomunicaciones es definir un servidor de syslog para que todos los logs sean enviados a él. Estos parámetros podemos definirlos en un router o switch de la empresa Cisco, aunque la gran mayoría de este tipo de dispositivos, de cualquier fabricante, permite estas configuraciones. Y es muy sencillo configurar un servidor syslog en cualquier sistema del tipo UNIX. Con los siguientes comandos podemos definir en un router o switch Cisco a qué servidor syslog le vamos a enviar los logs:

```
logging IP_o_Hostname
```

```
logging facility local7
```

```
logging on
```

El 51% de las empresas utiliza alguna solución para la administración de logs

(Fuente: CSI Computer Crime and Security Survey)

Figura 7. Fortinet es un fabricante de dispositivos de seguridad que cuenta con una gran reputación, y una muy buena relación de calidad y precio (www.fortinet.com).

The screenshot displays the Fortinet website interface. At the top, there's a navigation bar with links like 'Products', 'Solutions', 'Industries', 'How to Buy', 'Service & Support', 'Partners', and 'About Us'. The main banner features the headline 'THE SPEED YOU NEED' and describes the 'NEW FORTINET 5000-SERIES HIGH-SPEED BOARDS' as 'The world's fastest security and switching boards deliver up to 500 Gbps Firewall throughput'. Below this, there are several sections: 'CUSTOMER SPOTLIGHT' featuring Dunkley, Inc., 'NEWS COVERAGE' with a link to a story about Fortinet's 27th anniversary, 'ANALYST AWARD' from Gartner, and a 'FortiGuard Security Center' section. The bottom of the page includes a 'GUESS' section with a link to 'More Customer Success' and a 'Download Report' link.

FIREWALLS

El concepto de firewall ha cambiado mucho en los últimos años, y ha dejado de ser algo tan simple como filtrado por origen, destino y puertos, para pasar a abarcar equipos o aplicaciones muchísimo más granulares, que, incluso, llegan a inspeccionar el contenido de los paquetes que pasan a través de ellos e interpretan los protocolos utilizados para la comunicación. Es por eso que debemos aprovechar al máximo estas nuevas capacidades, para incluirlas dentro de nuestras medidas de protección.

Es preciso tener en cuenta si vamos a seleccionar un dispositivo del tipo UTM (**Unified Threat Management**), que contiene varias capacidades en un mismo equipo, como anti-virus, antispam, filtrado web, y muchas otras; o si vamos a optar por instalar un equipo para cada función importante. Esta es una de las cuestiones que se nos pueden presentar al llevar a cabo la tarea de diseñar las medidas de protección para una red.

La decisión que tomemos deberá estar basada en nuestras necesidades. Por ejemplo, en caso de que precisemos capacidades avanzadas de filtrado antispam, y vayamos a manejar una cantidad muy grande de correos electrónicos,

será recomendable contar con un dispositivo dedicado a estas tareas.

En cuanto a la selección del firewall que vamos a implementar, si bien muchos nuevos productos ofrecen muchísimas capacidades,

“el filtrado por origen, destino y puertos bloquea la mayor parte de los accesos malintencionados



Debemos considerar las otras características como adicionales, y evaluar si verdaderamente sacaremos provecho de ellas. Cabe destacar que, a mayor cantidad de características, mayor será la dificultad de administración y mantenimiento, además de que mayor será la probabilidad de que se presenten fallas en el dispositivo.

Con respecto a las configuraciones por defecto, y como debe hacerse en todos los dispositivos, los firewalls tienen que denegar todos los accesos que no hayan sido explícitamente permitidos. Esta regla también se conoce como *Deny by default* o **denegación por defecto**.

Es uno de los principios que nos permitirá mejorar nuestras tareas de todos los días, porque nos fuerza a conocer exactamente qué es lo que permitimos y por qué lo ha-

cemos. Por ejemplo, si debemos permitir que un equipo acceda a una aplicación remota, debemos permitir que solo ese equipo acceda únicamente a las direcciones y puertos que se van a utilizar para dicha aplicación, ni más ni menos.

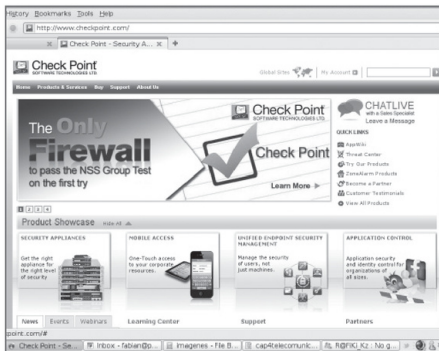


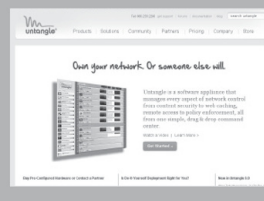
Figura 8. Checkpoint es uno de los fabricantes de dispositivos de tipo firewall más destacados en el mundo. Cuenta con excelentes productos y siempre es pionero en agregar nuevas características a sus equipos.

“

Al crear reglas de filtrado, es de suma importancia que lo hagamos de la forma más específica posible

RECOMENDADOS

Si no podemos contar con un *appliance* de seguridad, podemos optar por instalar algunas de las alternativas de código abierto, que han demostrado ser excelentes productos. Muchas de ellas ofrecen versiones pagas, que incluyen funciones adicionales. Algunos ejemplos son: **m0n0wall** (<http://m0n0.ch>), **IPCop** (www.ipcop.org) y **Untangle** (www.untangle.com). Para consultar una lista más completa y detallada, podemos visitar: http://en.wikipedia.org/wiki/List_of_router_or_firewall_distributions



41% de las empresas terceriza la administración de firewalls

(Fuente: KPMG Information Security Survey)

En caso de que no contemos con los recursos económicos para adquirir un dispositivo preparado específicamente para trabajar como un firewall, podemos utilizar un router o un servidor con alguna distribución de GNU/Linux o BSD. Las ventajas y desventajas de cada una de estas opciones se explican en el apartado "Diseño de redes seguras".

REDES INALÁMBRICAS

Otra de las nuevas comodidades tecnológicas requeridas en muchas organizaciones son las redes inalámbricas, que simplifican las conexiones al evitar la presencia de cables, aunque también aumentan el campo de conexión disponible para las personas mal intencionadas.

A diferencia de lo que muchas veces se cree, las redes inalámbricas pueden tener una muy buena seguridad, si se las configura correctamente. Cualquier información que circule por la red sin ser encriptada, puede ser fácilmente capturada por una persona que esté relativamente cerca de los dispositivos que transmiten y reciben los datos.

Las creencias de inseguridad en este tipo de redes se fundamentan, principalmente, en que los primeros protocolos de conexión no eran robustos y presentaban fallas que volvían muy fácil el ataque. En la actualidad, los protocolos se han mejorado y brindan excelentes características de seguridad.

Todas las vulnerabilidades que existen en las redes cableadas se aplican a las redes inalámbricas. Pero esto no funciona a la inversa, porque las redes inalámbricas presentan nuevos ries-

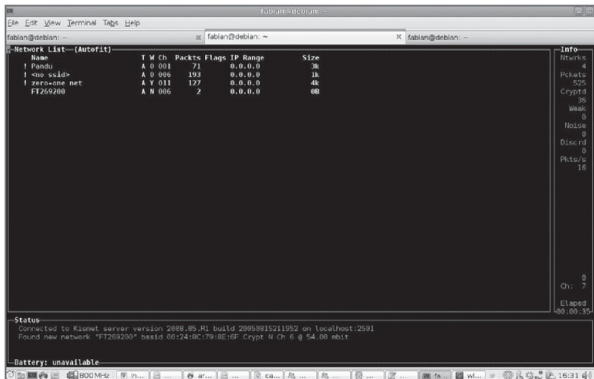


Figura 9. Aquí podemos ver cómo utilizamos la herramienta Kismet para conocer rápidamente cuáles son las redes inalámbricas que están a nuestro alcance. Hecho esto, podemos analizar más a fondo la configuración de cada una de ellas.

gos, al tener un medio de transmisión compartido por todos (el aire). Es por eso que debemos tener algunas consideraciones especiales, que podemos ver en la siguiente lista:

Modificar los SSID que vienen por defecto:

generalmente, los SSID que vienen por defecto brindan información acerca del punto de acceso que podría ser utilizado por un atacante para buscar vulnerabilidades.

No publicar el SSID en modo broadcast: esto hará que nuestra red no sea tan visible, aunque puede ser encontrada por programas especializados en detección de redes inalámbricas.

Modificar periódicamente las claves precompartidas: hará más difícil la tarea de crackear las claves, porque le dará menos tiempo al atacante para hallar la clave correcta.

Implementar métodos de autenticación

fuerte: contando con servidores LDAP o Radius para la autenticación, nos permitirá identificar fácilmente al usuario que está conectado a la red. También podemos utilizar smart cards y tokens.

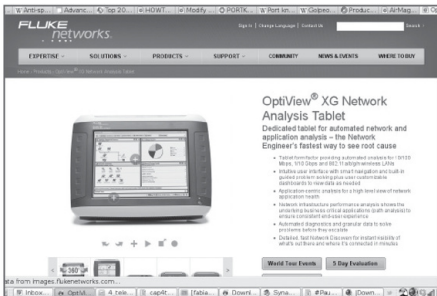
Utilizar WPA/WPA2 en lugar de WEP: es ampliamente conocido que la seguridad que ofrece

MUST KNOW

Debemos visualizar las redes inalámbricas como un tipo de red más, y dejar atrás el viejo mito de que utilizarlas significa hacer que nuestra red se vuelva totalmente vulnerable. Siempre tenemos que estar abiertos a implementar este tipo de conexiones, porque actualmente son necesarias para el buen funcionamiento de la mayoría de las organizaciones.

Figura 11.

FlukeNetworks ofrece una gran cantidad de productos para el análisis de redes inalámbricas. Desde software instalable en una PC, hasta un dispositivo del tipo tablet desarrollado particularmente para analizar este tipo de redes (www.flukenetworks.com).



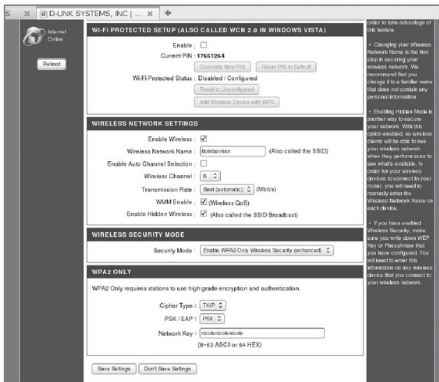
el protocolo WEP es casi nula. WPA y WPA2 brindan una mejor seguridad.

Implementar las últimas medidas disponibles.

este tipo de tecnologías evoluciona constantemente, así que debemos estar al tanto de

las nuevas capacidades que brindan nuestros equipos. Como podemos observar, muchas de estas medidas simplemente complican un poco la tarea de un atacante en su camino al éxito de romper la seguridad de una red. Es por eso que

Figura 12. En la captura de pantalla podemos ver cómo se encuentran configuradas algunas de las opciones de seguridad de la red inalámbrica en un router D-Link DIR-300. Algunas son WPA2, SSID oculto, el cifrado de tráfico y el protocolo PSK.



```

Home - PuTTY

Aircrack-ng 1.0

[00:00:18] Tested 1514 keys (got 30566 IVs)

KB    depth  byte(vote)
0     0/   9   1F(39680) 4E(38400) 14(37376) 5C(37376) 9D(37376)
1     7/   9   64(36608) 3E(36352) 34(36096) 46(36096) BA(36096)
2     0/   1   1F(46592) 6E(38400) 81(37376) 79(36864) AD(36864)
3     0/   3   1F(40960) 15(38656) 7B(38400) BB(37888) 5C(37632)
4     0/   7   1F(39168) 23(38144) 97(37120) 59(36608) 13(36352)

KEY FOUND! [ 1F:1F:1F:1F:1F ]
Decrypted correctly: 100%

```

Figura 12. Aircrack es un software de código abierto muy utilizado para romper la seguridad de redes WEP y WPA. Podemos utilizarlo para verificar qué tan difícil es acceder a nuestras redes inalámbricas. En la imagen, podemos ver cómo fue utilizado para encontrar la clave de una red, y ha tenido éxito. Además de Aircrack, el proyecto incluye algunas otras utilidades, como Airodump y Aireplay. (www.aircrack-ng.org)

“debemos seleccionar cuidadosamente las configuraciones, manteniendo un buen balance entre la seguridad y la usabilidad de la red

También es importante analizar periódicamente nuestra red en busca de dispositivos sospechosos o configuraciones débiles.

EN LA PRÁCTICA PROFESIONAL

Es habitual que los empleados conecten routers inalámbricos a la red cableada, con el objetivo de utilizar sus smartphones o PDAs. Al hacer esto, no suelen tener los recaudos de seguridad necesarios, y el resultado es una red inalámbrica insegura, que podría servir como puente para acceder a los recursos de la red de área local. Entonces, un atacante podría aprovechar para acceder a nuestros recursos con suma facilidad. Como el costo de los routers inalámbricos es bastante bajo, muchos empleados adquieren este tipo de equipos por su cuenta y los instalan en las oficinas sin notificarlo al personal técnico. Es por eso que debemos evitar que lo hagan, para lo cual podemos restringir los puertos de los switches, de modo que cada uno de los dispositivos conectados a ellos deba ser previamente autorizado.

Además, tenemos que escanear en forma periódica las redes inalámbricas disponibles para detectar redes sospechosas.

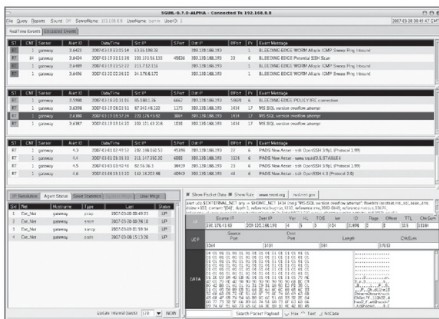


PREVENCIÓN DE INTRUSOS

Una de las tecnologías más avanzadas para proteger nuestras redes es la detección y prevención de intrusos, que nos permite trabajar de forma inteligente, analizando el tráfico y bloqueando los ataques automáticamente. Estos sistemas son complejos y puede llevar un tiempo configurarlos, pero son capaces de brindarnos un excelente nivel de seguridad al trabajar de forma automatizada y proactiva. La decisión de instalar o no este tipo de soluciones dependerá de la complejidad de la red, nuestros recursos y necesidades.

Los sistemas que solo pueden detectar ataques se conocen como Sistemas de Detección de Intrusos (IDS), y los que pueden tomar acciones para bloquear estos ataques se llaman Sistemas de Prevención de Intrusos (IPS). Obviamente, los IPS son bastante más complejos que los IDS, y requieren de mayor atención al configurarse, porque pueden bloquear tráfico legítimo e impactar negativamente en la operativa de la organización. Es común referirse a ambos tipos de sistemas, simplemente, como IDS, y así lo haremos a lo largo del libro.

Figura 13. Snort (www.snort.org) es el IDS de código abierto más reconocido. Cuenta con varios años de desarrollo y excelentes capacidades de detección. En la imagen podemos observar cómo se utiliza la interfaz Sguil para interpretar las alertas de Snort, en la que podemos ver varios ataques del tipo MS-SQL version overflow, como el que está señalado.



MUST KNOW

La implementación de este tipo de sistemas debe verse como opcional, debido a que no todas las organizaciones necesitan las tecnologías para prevención de intrusos. Antes de implementarlos, tengamos en cuenta todas las necesidades de nuestra organización y los recursos con los que contamos para llevar adelante un proyecto con estas características.

Muchos IPS permiten trabajar temporalmente como si fueran IDS, solo notificando los ataques detectados, lo que nos da la oportunidad de visualizar cómo funciona la solución y configurarla correctamente, para luego habilitar las capacidades de bloqueo. Esto es algo recomendable para iniciarnos en la configuración y puesta a punto de este tipo de sistemas.

Los IDS pueden estar basados en host (HIDS), que se instalan en un servidor para analizar el tráfico y las acciones realizadas dentro de él para detectar ataques, los cuales evaluaremos en el

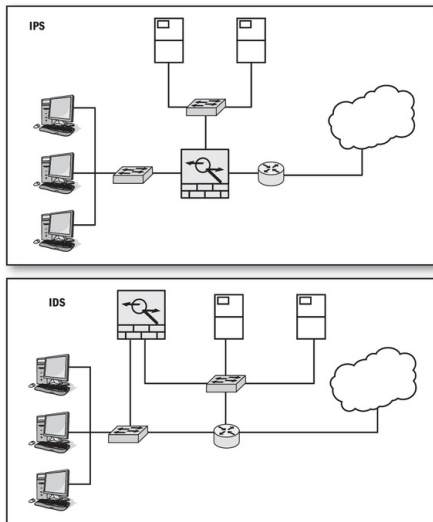


Figura 14. En el diagrama podemos observar claramente cómo un dispositivo del tipo IPS queda ubicado de forma tal que pueda tener la capacidad de bloquear conexiones, y entonces permitir o no el paso del tráfico. En cambio, un IDS queda ubicado por fuera de la red, y recibe el tráfico con el único objetivo de efectuar análisis y reportes.

siguiente capítulo. También pueden estar basados en red (NIDS), que se utilizan para analizar el tráfico de toda la red en busca de ataques entre dispositivos. Desde el punto de vista del funcionamiento, un IDS puede verse, simplemente, como

un analizador que reconoce distintos patrones de ataque, ya sea analizando un archivo de logs, un comportamiento del sistema operativo o las características de los paquetes enviados de un host a otro. Esto se debe a que, muchas veces,

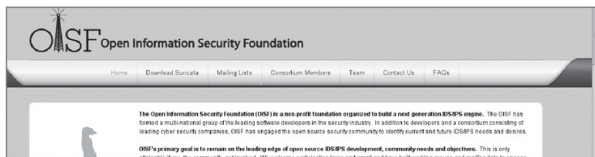


Figura 15. Suricata es un IDS de código abierto desarrollado por la **Open Information Security Foundation**, que implementa novedosas tecnologías de detección (www.openinfosecfoundation.com).

Este tipo de sistemas suele tener un costo elevado, por lo que recomendamos realizar una primera aproximación a estas soluciones a través de algún proyecto de código abierto (Snort puede ser la opción más viable). Una vez que hayamos realizado dichas pruebas, estaremos en una mejor posición para decidir si precisamos este tipo de sistemas y si vale la pena optar por una opción comercial, o si nuestras necesidades son cubiertas con el producto gratuito. Cualquiera sea la decisión, tengamos en cuenta que un sistema IDS puede facilitarnos todas nuestras tareas, y que podría ser una decisión inteligente asignar muchos recursos a instalar y mantener esta solución.

ADMINISTRACIÓN REMOTA

Una de las características más utilizadas por los administradores de red para simplificar su trabajo diario es el manejo remoto de los equipos de telecomunicaciones, lo que permite gestionar toda una red desde la comodidad de una única terminal. Este tipo de protocolos y herramientas son necesarios, pero deben ser utilizados y configurados con cuidado, porque suelen estar dentro de los principales intereses de una persona malintencionada que busque atacar nuestra red. Dependiendo del fabricante, cada dispositivo puede contar con varias interfaces de administración, como SNMP, SSH, interfaces web y protocolos propietarios. Es de suma importancia que utilicemos solamente protocolos que encripten el tráfico, como SNMPv3, SSH y HTTPS. Además, debemos tomar los recaudos necesarios acerca de la fortaleza de las contraseñas por utilizar.

De ser posible, es recomendable seleccionar un método de gestión que nos permita automatizar tareas de rutina, como lo son las copias de seguridad de configuraciones. Varios fabricantes cuentan con herramientas propias, que suelen limitarse a gestionar sus equipos.

Existen soluciones en el mercado compatibles con varios fabricantes. Si optamos por utilizar herramientas multi-fabricante, debemos verificar que sean soportados todos los equipos presentes en la infraestructura.

En el caso de los dispositivos Cisco, es recomendable habilitar la administración exclusivamente por SSH versión 2, bloqueando tanto la versión 1 de este protocolo como el protocolo 'telnet'.

Abajo vemos un ejemplo de cómo realizar esto:

```
crypto key generate rsa
```

```
ip ssh version 2
```

```
ip ssh on-retries 3
```

```
ip ssh logging events
```

```
line vty 0 4
```

```
transport input ssh
```

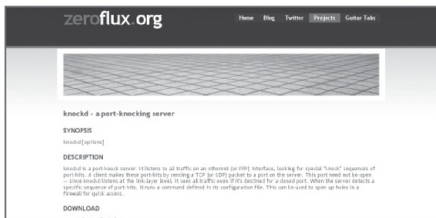
Con la siguiente configuración establecemos:

1. Generar las claves RSA para utilizar con SSH.
2. Utilizar solamente la versión 2 de SSH.
3. Permitir solamente tres intentos fallidos de conexión.
4. Guardar el registro de eventos de SSH.
5. Configurar las líneas vty 0-4.
6. Aceptar administración solo por SSH (produce el bloqueo de Telnet).

MUST KNOW

El hecho de que un dispositivo admita ser administrado en forma remota no tiene por qué implicar una vulnerabilidad. Simplemente, debemos configurar los accesos de la manera más segura posible, encriptando el tráfico, y permitiendo únicamente las conexiones desde equipos confiables. Así lograremos un buen balance entre seguridad y usabilidad.

Figura 16. El software de código abierto **RANCID** nos permite descargar automáticamente la configuración de nuestros dispositivos y almacenar un historial de versiones, que muestra las diferencias entre una y otra (www.shrubby.net/rancid).



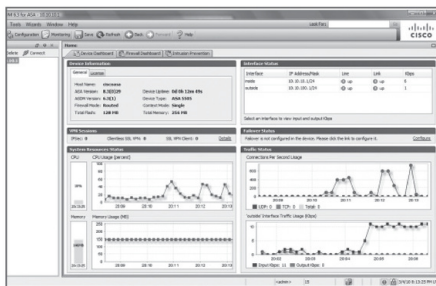
Al habilitar usuarios para poder acceder a los dispositivos y gestionarlos, es necesario tener en cuenta la implementación de permisos y perfiles, para que cada uno pueda acceder solo a las funciones que necesita para realizar sus tareas diarias. También es de suma importancia guardar un registro de todas las acciones realizadas sobre los equipos, de modo de poder analizar posteriormente cualquier anomalía o cambio de configuración no autorizado.

CLI VS. TUI VS. GUI VS. WUI

Existen varias formas de interactuar con un dispositivo o sistema. Hace muchos años, la

única manera disponible era a través de la línea de comandos o CLI (**Command Line Interface**). Con el correr del tiempo, se fueron desarrollando las TUI (**Text User Interface**), que, básicamente, son interfaces de texto un poco más amigables, con menús y ayuda por pantalla. Con la gran explosión de los entornos de escritorio, vinieron las GUI (**Graphic User Interface**), que presentaban ventanas, botones y nuevos componentes que hacen más fácil la interacción para el usuario. En los últimos años se han puesto muy de moda las WUI (**Web User Interface**), muy similares a las GUI, pero a las que se accede a través de un servidor web. Hecha esta pequeña diferenciación de términos,

Figura 17. ASDM es una herramienta desarrollada por Cisco, que ofrece la capacidad de gestionar sus dispositivos de seguridad. El cliente se ejecuta sobre plataformas Microsoft Windows. En la imagen se muestran algunos de los datos que aparecen en el panel principal, como las sesiones VPN, el tráfico, el consumo de recursos y el estado de las interfaces de red. (www.cisco.com)



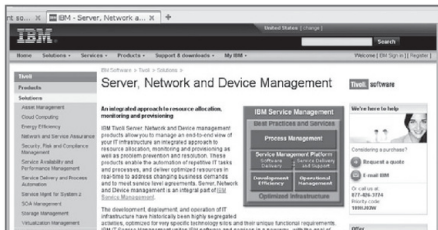


Figura 18. IBM Tivoli es un software avanzado que permite gestionar nuestros dispositivos de telecomunicaciones, servidores y otro tipo de equipamiento (www.ibm.com).

podemos decir que, actualmente, en el caso de los sistemas que están pensados para ser accedidos por personas con altos conocimientos tecnológicos, aún predominan las interfaces por línea de comandos. Si bien es cierto que la mayoría de dichos sistemas cuenta con GUI o WUI, estas no ofrecen la misma cantidad de opciones que las CLI. Por ejemplo, en los routers y firewalls, es muy común que las opciones más importantes y de uso frecuente estén disponibles dentro de la configuración por interfaz gráfica, pero existe un número de opciones avanzadas y de uso no muy frecuente que solo pueden ser accedidas a través de la línea de comandos. Por lo tanto, es ampliamente recomendable que nos familiaricemos con este tipo de interfaces. Aunque no vayamos a utilizarlas en nuestras tareas diarias, además de presentar opciones que no están disponibles a

través de otras interfaces, suelen estar disponibles siempre, porque son muy simples. Por el contrario, las interfaces GUI y WUI pueden ser inaccesibles en ciertas circunstancias.

Por último, otra de las grandes ventajas de las CLI es que nos permiten automatizar tareas fácilmente, a través de lenguajes de **scripting** como **Python**, **Perl** y **Ruby**. Esto nos permitirá, por ejemplo, realizar funciones de backup, reportes o tareas de mantenimiento de forma programada y sin interacción del personal.

PROTOCOLOS TCP/IP

Además de los protocolos IP, TCP, UDP e ICMP, la suite de protocolos TCP/IP contiene otros componentes fundamentales en las arquitecturas de red de todo el mundo. Es por eso que debemos prestarles especial atención y conocerlos a fondo

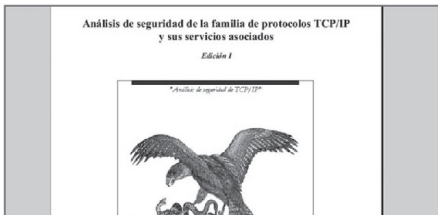
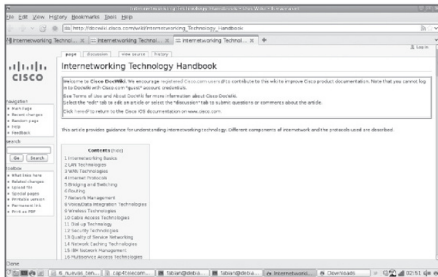


Figura 19. Este libro gratuito, escrito por Raúl Siles Peláez, hace un análisis de seguridad del conjunto de protocolos TCP/IP. Se encuentra disponible en www.portantier.com.

Figura 21. El sitio wiki de Cisco alberga un interesante documento llamado **Internetworking Technology Handbook**, que explica los protocolos relacionados con las redes y su funcionamiento (http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook).



si pretendemos ser verdaderos profesionales de la seguridad. Algunos de los protocolos que seguramente utilizamos dentro de nuestra organización son DHCP, DNS, SSH, HTTP, FTP, SMTP, POP3, IMAP, SNMP y SSL/TLS. A continuación, analizaremos cada uno de ellos.

SSH

Secure Shell es el nombre tanto del protocolo como del programa que lo implementa, y sirve para acceder a los dispositivos a través de la red. Es un reemplazo para el protocolo Telnet, que

presentaba varias vulnerabilidades. Además, cuenta con diversas capacidades avanzadas, como copiar archivos y redirigir el tráfico a otras aplicaciones, para crear un túnel seguro. Es muy habitual usarlo para acceder a servidores UNIX y dispositivos de red como routers, switches y firewalls. La versión recomendada es la 2, porque la 1 presenta algunas vulnerabilidades graves. Es de suma utilidad saber utilizar este protocolo, las herramientas y las capacidades adicionales que posee. Se encuentra disponible para gestionar tanto dispositivos de red como sistemas operativos UNIX.



Figura 21. OpenSSH es la implementación de SSH más utilizada en el mundo. En el sitio web del proyecto podemos encontrar gran cantidad de información de interés; está en: www.openssh.com.

En el siguiente código podemos observar cómo se utiliza el estilo comando 'scp' (incluido en el proyecto OpenSSH) para realizar la transferencia de archivos entre servidores, empleando canales encriptados. Se puede ver claramente cómo se empleando claves criptográficas RSA para la autenticación de los equipos.

```
fabian@debian:~$ scp 192.168.0.115:/archivo.txt ./
Authenticity of 192.168.0.115 can't be established
RSA key fingerprint is 01:18:46:a8:02:37:dc:6b:e3:dd:e2:ba:c8:0c:bb:44.
Are you sure you want to continue(yes/no)? yes
Added '192.168.0.115' to the list of known hosts.
fabian@192.168.0.115's password:
archivo.txt 100% 0 0.0KB/s
00:00
```

Además de scp, podemos utilizar herramientas de entorno estilo comando gráfico, mucho más amigables, como WinSCP (<http://winscp.net>).

TLS

Transport Layer Security y su predecesor, **Secure Socket Layer** (SSL) nos dan la posibilidad de agregar una capa de seguridad a otros

protocolos. Utiliza una mezcla de criptografía simétrica y asimétrica para garantizar la privacidad e integridad de los datos. Suele ser de mucha utilidad para proteger protocolos como HTTP y SMTP, que no fueron desarrollados para proteger los datos que intercambian. Aunque debemos recordar que el hecho de proteger el tráfico encriptándolo no nos libera de otro tipo de ataques, como la fuerza bruta, los exploits, y otros.

Entre 2008 y 2009 los ataques de capturas de contraseñas crecieron un 88%

(Fuente: CSI Survey 2009)

SMTP, IMAP Y POP3

Estos tres protocolos son los más utilizados por las arquitecturas de correo electrónico. El primero, **Simple Mail Transfer Protocol**, sirve para transportar los mensajes de correo. Los dos últimos, **Internet Message Access Protocol** y **Post Office Protocol 3**, son empleados para que los usuarios accedan a los correos que están alojados en los servidores. Como la mayoría de los protocolos TCP/IP, estos tres envían y reciben la información en texto plano, por lo que son muy vulnerables a

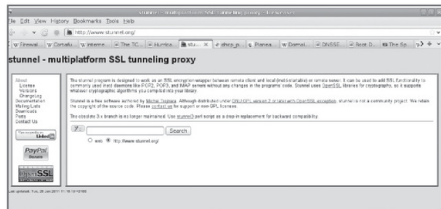


Figura 22. Stunnel nos permite proteger aplicaciones utilizando TLS. Puede ser de mucha utilidad para dotar a nuestros programas o servicios inseguros de una buena capa de seguridad, sin requerir mayores esfuerzos (www.stunnel.org).

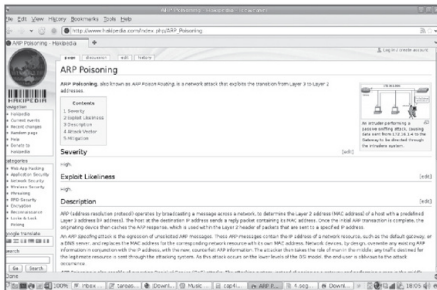
MUST KNOW

Debemos analizar constantemente nuestra red en búsqueda de protocolos extraños o no permitidos, debido a que es posible conocer qué herramientas o software están utilizando los servidores y estaciones de trabajo si sabemos qué tipo de datos. Son varias las aplicaciones malintencionadas que generan ciertos patrones de tráfico detectables.

las capturas de tráfico. Actualmente, muchos de los servicios más populares de correo soportan el uso de TLS para proteger a estos protocolos (que en su versión segura se llaman SMTPS, IMAPS y POP3S). Es ampliamente recomendable emplear las versiones seguras de ellos.

En el caso de SMTP, además de la encriptación de tráfico, es importante utilizar medidas de seguridad para bloquear los intentos de enviar spam a través de nuestros servidores. Esto es particularmente importante porque podríamos terminar en las listas negras y nuestros servidores serían bloqueados, lo que causaría la pérdida de varios correos.

Figura 23. Hakipedia (www.hakipedia.com) es un sitio web del tipo wiki en el cual podemos encontrar descripciones de varias clases de ataque. Es un excelente recurso de información para mantenernos actualizados. En la imagen podemos ver el artículo que describe los ataques del tipo ARP Poisoning.



Las técnicas y mejores prácticas para luchar contra el spam se discuten con más detalle en el **Capítulo 6**.

```
fabian@debian:~$ telnet smtp.gmail.com 25
Trying 74.125.159.109...
Connected to gmail-smtp-msa.l.google.com.
Escape character is '^J'.
220 mx.google.com ESMTP
HELO fabian
250 mx.google.com at your service
MAIL FROM: fabian@portantier.com
530 5.7.0 Must issue a STARTTLS command first.
```

En el código anterior, podemos ver cómo al intentar enviar un correo, los servidores de Gmail nos obligan a utilizar TLS para autenticarnos y encriptar las comunicaciones.

HTTP Y FTP

Hyper Text Transfer Protocol y **File Transfer Protocol** son los protocolos utilizados habitualmente para transferir archivos y documentos a través de las redes. El uso más frecuente de HTTP es servir las páginas de los sitios web.

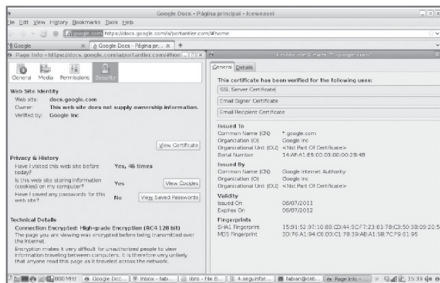


Figura 24. En la imagen podemos ver los detalles del certificado TLS que utiliza Google para su servicio Google Docs. Algunos de los datos interesantes son los algoritmos de encriptación (RC4 128 bits) y la cantidad de veces que se ha visitado el sitio, que indican que no hubo modificaciones en el certificado TLS desde la primera visita que realizamos.

Tanto HTTP como FTP envían y reciben los datos en texto plano, lo que los hace muy inseguros si necesitamos transferir información confidencial o credenciales de acceso.

En el caso de HTTP, existen dos formas para solicitar credenciales de autenticación: Basic y Digest. En la primera, el usuario y la contraseña se envía directamente sin encriptar, por lo que es fácilmente capturable. Con respecto al método Digest, se utiliza encriptación para transmitir las credenciales. Aun así, podemos ser víctimas de un ataque del tipo *Man-in-the-middle* (que consiste en que un atacante se interponga entre el cliente y el servidor, capturando y hasta modificando el tráfico entre ambos), debido a que no se valida al cliente en sí. Además, solo se están

protegiendo las credenciales enviadas, y no, los datos que pueden ser transferidos después. Evidentemente, la seguridad de estos dos protocolos es muy pobre, y es por eso que se recomienda utilizar TLS para agregar encriptación y autenticación del cliente. Las versiones de dichos protocolos se conocen como HTTPS y FTPS. En el caso de FTP, podemos considerar la opción de reemplazarlo por SFTP, que es un método de transferencia de archivos que utiliza SSH para brindar seguridad en nuestros datos.

DHCP

Dynamic Host Configuration Protocol permite a los clientes de una red obtener sus parámetros



Figura 25. La herramienta DHCP-Probe (www.net.princeton.edu/software/dhcp_probe) nos permite detectar los servidores DHCP que se encuentran en una red local. Es de mucha utilidad para detectar servidores que no deberían estar ahí.

Figura 26. El Internet Systems Consortium (www.isc.org) desarrolla, entre otros, el famoso servidor de DNS de código abierto BIND. También mantiene software de cliente y servidor DHCP. Es un excelente sitio web en el que buscar información acerca de estos protocolos.



de configuración automáticamente. Aunque en general se utiliza solo para que los clientes obtengan la información de dirección IP, puerta de enlace y servidores DNS, el protocolo tiene muchas más opciones y parámetros. Como es un protocolo que fue desarrollado para ser muy simple, también es muy inseguro. Un atacante podría utilizar nuestros servidores DHCP para obtener una dirección de red válida y consultar información de la red. También es sencillo crear un servidor DHCP para confundir a los otros clientes de la red, o generar un pequeño programa que envíe múltiples peticiones al servidor, haciendo que las direcciones disponibles para asignar se agoten. Para evitar ataques, la mejor opción es monitorear los registros de sistema a fin de detectar comportamientos extraños. También debemos estar alertas acerca de la cantidad de direcciones sin asignar de las que disponemos. Es una excelente idea monitorear la red un busca de servidores DHCP adicionales. Otra medida de seguridad muy habitual es definir una lista de direcciones MAC a las cuales responderá nuestro servidor DHCP, y hacer que se registren como

alertas las peticiones que vengan de direcciones MAC que no estén en esa lista. Cabe destacar que varios de estos problemas de seguridad son solucionados con el uso de IPv6.

DNS

Domain Name System se utiliza, entre otras cosas, para que las computadoras puedan resolver nombres de dominio a direcciones IP. También es usado para determinar cuáles son los servidores SMTP que corresponden a un determinado dominio. Los servidores DNS representan una pieza crítica de la infraestructura de las redes e Internet. Si un atacante consigue tomar el control de nuestros servidores DNS, tiene la posibilidad de realizar varios subataques con grandes probabilidades de éxito, como, por ejemplo, el **phishing**. Particularmente, el diseño del protocolo DNS no presenta mayores inconvenientes de seguridad, pero debemos prestar especial atención a este tipo de servidores con respecto a una mala configuración, que podría exponer información confidencial de nuestra organización y los dominios de los cuales somos responsables.

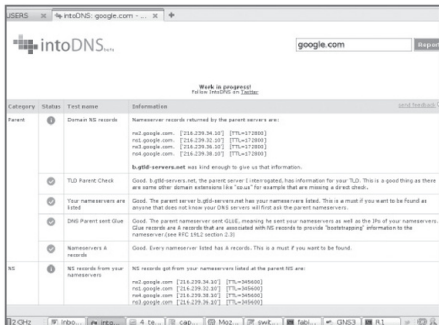


Figura 27. Existen varios sitios web que nos permiten comprobar errores en la configuración de los DNS de un dominio de forma rápida y gratuita. Algunos de ellos son: www.intodns.com, www.dnscolors.com, www.dnsssy.com y www.dnscog.com.

SNMP

Simple Network Management Protocol se utiliza, habitualmente, para consultar o modificar información en los dispositivos de telecomunicaciones, como routers, switches y firewalls, aunque también existen versiones disponibles para UNIX y Windows.

Ofrece una manera fácil de acceder a la información del equipo y a cada una de sus interfaces. La mayoría de las herramientas de monitoreo lo utilizan en mayor o menor medida.

```
snmp-server view ReadView system included
snmp-server group ReadOnly v3 auth read
ReadView
snmp-server user fabian ReadOnly v3 auth
md5 mipassword priv des56 pfpfpf
```

Con el comando de arriba "(para dispositivos CISCO)" hacemos lo siguiente:
Creamos la vista **ReadView**, que solamente puede leer los atributos dentro de **system**.
Creamos el grupo **ReadOnly**, de **SNMPv3**, con la vista **ReadView**.

Creamos el usuario **fabian**, del grupo **ReadOnly**, de **SNMPv3**, con la contraseña **mipassword**, encriptada con **MD5** y el tráfico encriptado con **DES56**, utilizando la clave **pfpfpf**.

Para verificar nuestra configuración, podemos utilizar los siguientes comandos:

```
show snmp view
show snmp group
show snmp user
```

MUST KNOW

Cada uno de estos protocolos de red cuenta con sus recomendaciones de seguridad correspondientes, que evitan una gran cantidad de vulnerabilidades y posibles ataques. Es de vital importancia que verifiquemos nuestras configuraciones y busquemos alinearlas con las mejores prácticas internacionales y las guías del fabricante de nuestros productos.

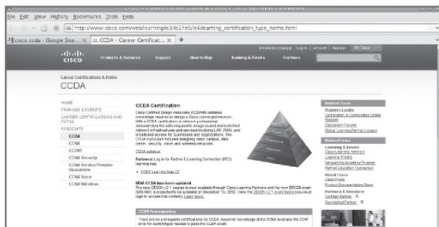


Figura 29. Cisco Systems ha creado varios niveles de certificación para profesionales del diseño de redes (CCDA, CCDP, CCDE), lo cual muestra la importancia de este tipo de conocimientos.

la capacidad de construir la red desde cero y, en caso de que estemos trabajando con una red ya construida, analizar cómo podemos mejorarla constantemente.

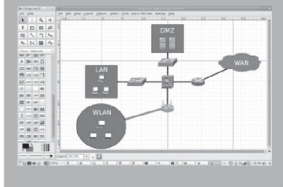
Llevando el ejemplo al extremo, la red más insegura es aquella que se denomina "plana", en

la cual todos los equipos tienen conectividad abierta entre unos y otros, sin ningún tipo de filtrado. En este caso, la seguridad quedaría relegada únicamente a las estaciones de trabajo y los servidores, que deberían protegerse cada uno por su cuenta. Como vimos anteriormente, el concepto de "defensa en profundidad" nos lleva a implementar varios controles en todos los puntos que nos sea posible. Así que debemos prestar mucha atención a las opciones de seguridad que ponen a nuestra disposición los dispositivos de telecomunicaciones.

“ Debemos tener en cuenta que una conexión que no puede realizarse no puede ser utilizada para atacar a un sistema

EN LA PRÁCTICA PROFESIONAL

Es una excelente idea utilizar programas como Dia (mostrado en la imagen) o Microsoft Visio para diseñar diagramas que reflejen la topología de la red actual y actualizarlos regularmente. Esto no será de ayuda tanto para resolver problemas rápidamente, como para evaluar cambios y posibles mejoras en nuestra infraestructura. Debemos completar estos diagramas con todos los datos que nos sean de utilidad, como tipo de equipo, dirección IP, fabricante, etc.



RECOMENDADOS

Cisco SAFE (www.cisco.com/go/designzone) ofrece guías y documentos que dan varias recomendaciones para el diseño de redes seguras. Si bien están desarrolladas sobre la base del equipamiento fabricado por Cisco Systems, forman un excelente recurso para cualquier profesional que busque aprender cuestiones de diseño de redes seguras.

Entonces, es mucho más sencillo filtrar conexiones que intentar protegerlas con métodos complejos.

ZONAS DESMILITARIZADAS

También conocidas como DMZ, sirven para ubicar dispositivos que presten servicios públicos a través de Internet. Estos servicios, por naturale-

za, se encuentran mucho más expuestos que los utilizados solamente para propósitos internos. En caso de que, por ejemplo, un atacante pueda tomar el control de nuestro servidor web, esta separación complicaría el acceso desde allí hacia la red local (LAN). Por lo tanto, es necesario implementar este tipo de separaciones siempre que contemos con servidores expuestos a redes públicas, como Internet. También es recomendable utilizarlas para colocar los equipos destinados a conexiones con organizaciones asociadas, clientes o proveedores.

Estas separaciones pueden crearse utilizando firewalls, routers o un servidor dedicado a esta tarea. Entre todas estas opciones, cada una tiene sus ventajas y desventajas, de las cuales mencionamos algunas en el siguiente apartado.

FIREWALL

Es la opción más recomendable en todos los casos, sobre todo, porque se trata de equipos ya preparados para esta tarea y suelen contar

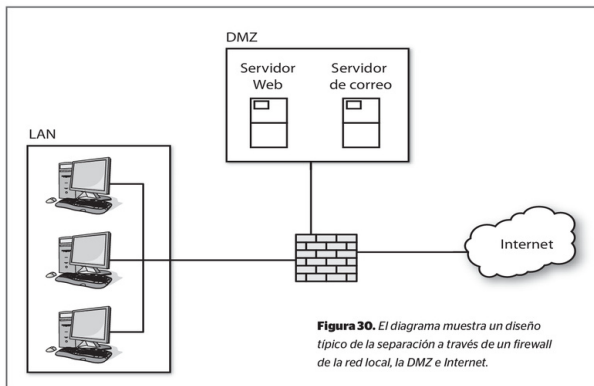


Figura 30. El diagrama muestra un diseño típico de la separación a través de un firewall de la red local, la DMZ e Internet.

Policy									
Create New: ▾		[Column Settings]							
Status	ID	Source	Destination	Schedule	Service	Profile	Action		
▼ internal -> wan1 (2)									
☒	2	all	all	always	ANY	scan	ACCEPT		
☒	5	localLAN	LondonLAN	always	ANY	scan	ENCRYPT		
▼ wan1 -> internal (2)									
☒	3	all	Exchange server	always	HTTP HTTPS IMAP SMTP POP3 ICMP_ANY	scan	ACCEPT		
☒	4	all	Exchange Discovery	always	HTTPS	scan	ACCEPT		

Figura 31. En la imagen podemos ver una captura de pantalla de la interfaz de configuración web de un equipo Fortigate, de la empresa Fortinet. Como podemos observar, presenta una interfaz sencilla, pero al editar cada una de las políticas, podemos configurar opciones avanzadas, como detección de Malware e IDS.

con opciones que nos serán de mucha utilidad. Algunos nos permitirán implementar controles antivirus y capacidades de NIDS, que van a reforzar mucho la seguridad entre la LAN y la DMZ. Además, suele ser la opción más sencilla de administrar, mantener y monitorear.

ROUTER

En caso de que no contemos con un firewall, podemos optar por utilizar un router y configurar una buena cantidad de listas de control de acceso, para tener bien limitado el tipo de conexiones que pueden realizarse de un lugar a otro. Con estos filtros bien configurados, podemos tener un buen nivel de seguridad, sin entrar en los costos que puede representar un firewall. A continuación

podemos ver un ejemplo de listas de control de acceso (ACL) en un router Cisco, que solamente permite tráfico DNS, HTTP, SMTP y POP3.

```
access-list 102 permit tcp any any eq www
access-list 102 permit tcp any any eq smtp
access-list 102 permit tcp any any eq pop3
access-list 102 permit udp any any eq domain
access-list 102 permit udp any eq domain any
access-list 102 permit tcp any any eq domain
access-list 102 permit tcp any eq domain any
```

SERVIDOR

Esta es una opción que puede resultar interesante, sobre todo, para los profesionales que cuenten con experiencia en sistemas operativos de código abierto, como GNU/Linux y BSD. Podemos instalar alguna de las distribuciones que están desarrolladas específicamente para ser utilizadas como firewalls. Puede ser la opción más económica, pero debemos tener en cuenta los problemas de disponibilidad que podemos llegar a tener en caso de que el servidor presente una falla de hardware.

Al seleccionar la opción que vamos a utilizar, es preciso tener en cuenta tanto nuestras capacidades económicas, como nuestras necesidades y conocimientos técnicos para llevar adelante la solución. Debemos considerar que, como la ma-

MUST KNOW

Debemos prestar atención a las separaciones de red tanto físicas como lógicas, manteniendo dos diagramas de topología distintos. Debido a que cada una de ellas representa diferentes medidas de seguridad, siempre hay que tener en cuenta que una separación lógica puede fallar por cuestiones de configuración, pero una física no.

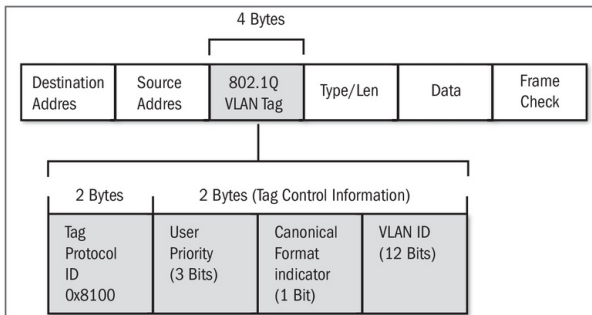


Figura 32. El diagrama nos muestra la manera en que se agregan 4 bytes a la trama Ethernet para los campos del protocolo 802.1Q.

yoría de las conexiones permitidas serán desde la LAN hacia la DMZ por propósitos de gestión de los equipos, no es estrictamente necesario contar con capacidades avanzadas de filtrado.

SEPARACIÓN DE VLANS

Virtual Local Area Network es un método para crear redes lógicamente independientes dentro de una misma red física. Para realizar esto, los paquetes son marcados con un campo especial, denominado etiqueta o tag, que identifica a las distintas VLANs. Dicho tag se ubica como un campo adicional en la estructura de datos de cada paquete transmitido. Esto nos permite tener el tráfico separado por medio de los switches y filtrar la conectividad entre los dispositivos, aunque se encuentren compartiendo un mismo medio físico. El estándar que actualmente se utiliza en la mayoría de las implementaciones de VLANs es el IEEE 802.1Q. Entre algunas de las ventajas que nos brinda tener nuestro tráfico separado por VLANs, pode-

mos enumerar los siguientes:

- » Delimitar los dominios de broadcast, para mejorar el rendimiento.
- » Organizar mejor la red y los dispositivos que están conectados a ella.
- » Disminuir la posibilidad de accesos no autorizados y escuchas de tráfico.

Como podemos notar, es de utilidad implementar separación de VLANs no solamente para propósitos de seguridad, sino también para mejorar el rendimiento de nuestra red. Esta es una capacidad con la que cuentan todos los switches actuales, tanto de fabricantes reconocidos, como de segundas marcas. Es ampliamente recomendable clasificar los tipos de tráfico que tendremos en nuestra red y, sobre esa base, definir distintas VLANs. En general, la clasificación adecuada estará basada en sectores de la organización, y podrá ser, por ejemplo: Finanzas, Marketing, Atención al cliente, Servidores, etc. También debemos tener en cuenta que ciertas tecnologías tienen requerimientos específicos en cuanto al rendimiento de la red; sobre todo, las tecnologías para transmisión de audio y video. Es por esto que se recomienda utilizar una VLAN dedicada para este tipo de tráfico.

“Es de suma importancia reservar una VLAN para la administración de dispositivos,

es decir, protocolos SNMP, SSH, etc. Esto nos permitirá conservar la gestión de los equipos, aun cuando la red esté saturada. Mantener este tipo de tráfico dividido del resto también nos servirá para implementar filtros más granulares acerca de qué estaciones de trabajo pueden administrar re-

motamente los dispositivos de red. En el siguiente ejemplo, veremos una configuración de VLANs de un equipo Cisco Catalyst 2924 XL, en la que separemos el tráfico de voz sobre IP (VoIP) de los tráficos de estaciones de trabajo y servidores.

```
vlan database
(vlan)#vtp transparent
Setting device to VTP TRANSPARENT mode.
(vlan)#vlan 10 name Workstations
VLAN10 added:
  Name: Workstations
(vlan)#vlan 20 name Servers
VLAN20 added:
  Name: Servers
(vlan)#vlan 30 name VoIP
VLAN30 added:
  Name: VoIP
(vlan)#exit
APPLY completed.
Exiting....
```

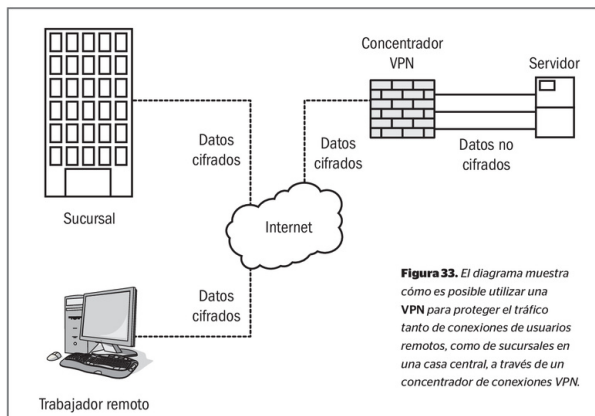


Figura 33. El diagrama muestra cómo es posible utilizar una VPN para proteger el tráfico tanto de conexiones de usuarios remotos, como de sucursales en una casa central, a través de un concentrador de conexiones VPN.

RECOMENDADOS

Algunas de las herramientas de VPN de código abierto más populares, que pueden ser instaladas en los sistemas operativos UNIX para funcionar como concentrador son: **OpenSSH** (www.openssh.com), **OpenVPN** (<http://openvpn.net>) y **FreeS/Wan** (www.freeswan.org).

REDES PRIVADAS VIRTUALES

Las conexiones VPN (*Virtual Private Networks*) deben ser utilizadas siempre que necesitemos realizar conexiones seguras sobre medios no seguros (internet). Este tipo de herramienta es de suma utilidad para habilitar el trabajo remoto y permitir que los empleados de la organización se conecten a nuestra red desde sus hogares u otros sitios. También es útil para conectar varias sucursales a una casa central.

Muchos de los dispositivos UTM pueden funcionar como concentradores de VPN, y los sistemas operativos UNIX cuentan con herramientas para el mismo propósito, generalmente, utilizando protocolos como IPSec y SSL/TLS, con algoritmos de encriptación como AES y 3DES y funciones de hash como MD5 y SHA. Cualquiera sea la combinación de estas herramientas, nuestras conexiones permanecerán relativamente seguras, con la única vulnerabilidad de que las credenciales de acceso puedan ser adivinadas o conseguidas por medios que no tengan que ver con la conexión VPN en sí.

PARA PONER A PRUEBA

1. ¿Por qué debemos prestar atención a la seguridad de routers y switches?
2. ¿Qué diferencia podemos encontrar entre los sistemas IDS e IPS?
3. ¿Para qué sirve la tecnología Port Security?
4. ¿Cómo podemos proteger el tráfico de los protocolos que envían los datos en texto plano?
5. ¿Qué dispositivos nos permiten dividir la red tipo LAN de la DMZ?

CAPÍTULO 5

SISTEMAS OPERATIVOS

PARA APROVECHAR ESTE CAPÍTULO

- » **INVESTIGAR** MÁS A FONDO CADA UNA DE LAS TECNOLOGÍAS EXPUESTAS.
- » **DESCARGAR** Y PROBAR EL SOFTWARE MENCIONADO.
- » **ACCEDER** A LAS GUÍAS DE SEGURIDAD PROVISTAS POR EL FABRICANTE DE NUESTROS SISTEMAS OPERATIVOS.

SISTEMAS OPERATIVOS

En este capítulo aprenderemos a:

Objetivo 1 Seleccionar y asegurar sistemas operativos.

Objetivo 2 Utilizar los protocolos de gestión adecuados.

Objetivo 3 Entender los distintos tipos de autenticación.

Los **sistemas operativos** representan un alto valor, tanto para las organizaciones como para sus posibles atacantes. Esto se debe, principalmente, a que son los encargados de almacenar y procesar la información, lo que hace que una falla en ellos puede ser causa de pérdida de datos, robo de datos y otros problemas serios. Como todas las tecnologías, estos sistemas han evolucionado constantemente, y se volvieron más seguros con el correr de los

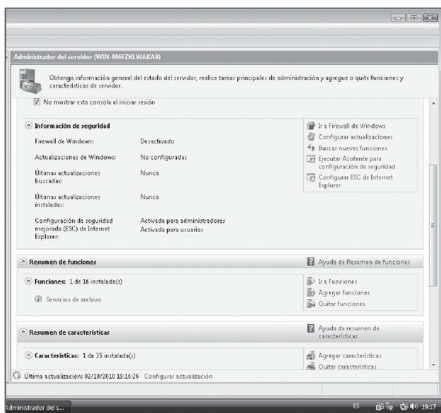


Figura 1. Windows Server 2008 muestra grandes mejoras de seguridad con respecto a sus versiones anteriores.

años. Pero también tuvieron que adaptarse a las nuevas necesidades del mercado, aumentando las capacidades de conectividad y la diversidad de las funcionalidades prestadas, lo cual abre las puertas a nuevos tipos de ataques y vulnerabilidades. Es por eso que podemos afirmar que, si bien los sistemas operativos son cada vez más seguros en su diseño, presentan cada vez mayores vectores de ataque, por estar obligados a ofrecer cada vez más funcionalidades.

Recordemos que, a mayor funcionalidad de un sistema, mayores son sus posibilidades de falla. Por otra parte, podemos observar que el mercado se vuelve más exigente en cuanto a los niveles de seguridad esperados, por lo que vemos que se implementan varias tecnologías desarrolladas exclusivamente para proteger los sistemas.

Este tipo de enfoque nos permite tener un mayor control de la seguridad, pero también nos obliga a estar al tanto de todas las capacidades con las que cuentan nuestros sistemas, para poder implementarlas correctamente. En la actualidad, existen varios tipos de sistemas operativos, para diferentes propósitos, aunque podemos afirmar que la mayoría de las instalaciones en empresas pertenecen a dos grupos: **Windows** y **UNIX**. En el primer caso, podemos encontrar sistemas tanto para escritorio (**Windows XP, Windows 7**) como para servidor (**Windows Server 2003, Windows Server 2008**).

En el segundo grupo, hay una infinidad de variantes —como **GNU/Linux, BSD, HP-UX, IBM-AIX, Solaris**, etcétera—, que suelen utilizarse, principalmente, para servidores.

Si bien cada sistema operativo tiene sus particularidades que lo vuelven único, los integrantes de cada uno de estos grupos mantienen grandes similitudes, por lo que hablaremos de sistemas Windows y sistemas UNIX, sin entrar en detalles minuciosos.

WINDOWS VS. UNIX

En este pequeño apartado intentaremos definir un tema que se viene discutiendo hace años, y hasta llegó a conocerse como la “guerra santa” del mundo informático. Nos referimos a la rivalidad entre los sistemas operativos de **Microsoft**, que son ampliamente los más utilizados del mundo, y los **UNIX**, que se dice que son los más seguros.

“Como profesionales, debemos dejar de lado cualquier preferencia que tengamos y ser objetivos a la hora de seleccionar el mejor sistema operativo para nuestros equipos

Las falencias de los sistemas Windows han sido muchas y muy graves, aunque, principalmente, esto estaba relacionado con el escaso interés de Microsoft por el tema seguridad. Actualmente, esta postura ha cambiado, y podemos observar que las nuevas versiones de Windows hacen mucho más hincapié en este aspecto. Muchos apoyan el diseño de los sistemas operativos UNIX, porque sostienen que están

desarrollados desde un punto de vista más organizado y simplista. Pero, como ya mencionamos, esta es una cuestión personal y, sobre todo, depende de las necesidades del momento. Objetivamente, cada tipo de sistema

EN LA PRÁCTICA PROFESIONAL

Tanto los sistemas operativos Windows como los UNIX cuentan con una gran cuota de mercado y son respetables, por tener varios años de desarrollo y una gran cantidad de software disponible. Es por eso que es habitual el hecho de encontrar una mezcla de ambos en todas las infraestructuras tecnológicas actuales. Como buenos profesionales, debemos tener un amplio conocimiento de ambos sistemas. Aunque no es necesario que seamos expertos en los dos (tarea que resultaría muy difícil), debemos tener la capacidad, por lo menos, de instalarlos, administrarlos y configurarlos correctamente, conociendo las ventajas y desventajas de cada uno, así como también las herramientas que podemos utilizar en cada sistema para aumentar su seguridad. Esto es algo

que, verdaderamente, va a distinguirnos en el mercado laboral, no solo porque tendremos la capacidad de trabajar con los dos, sino también porque el manejo de ambos nos permitirá tener una visión más amplia de los sistemas operativos en sí.



operativo tiene sus ventajas y desventajas, con lo cual la elección de uno u otro estará estrictamente relacionada con el propósito del sistema. Existe una infinidad de comparativas entre estos dos tipos de sistemas, así que no vamos a reinventar la rueda en este libro.

CONSEJOS PARA SISTEMAS WINDOWS

Este tipo de sistemas suele ser fácil de utilizar, pero no debemos dejar que esto nos lleve a subestimarlos. En sus últimas versiones, podemos apreciar que existe una gran cantidad de herramientas destinadas a aumentar la seguridad, muchas incluidas en la instalación por defecto y otras que pueden descargarse desde el sitio web del fabricante.

Hasta el día 11 de mayo de 2011, Microsoft Windows Server 2008 llevaba reportadas 320 vulnerabilidades

(Fuente: NIST National Vulnerability Database, <http://web.nvd.nist.gov>)

Siempre debemos prestar mucha atención a las nuevas notificaciones de seguridad y a los parches disponibles. Microsoft mantiene varios canales de comunicación para notificar a los usuarios y administradores acerca de las novedades en seguridad: desde la información básica para estar al tanto de las cosas, hasta temas más avanzados, dirigidos a administradores y pensados para darnos tiempo a preparar las acciones de aplicación de parches. También podemos encontrar un blog oficial, en el que se ofrecen contenidos referidos a varios tópicos de seguridad. Todos estos recursos pueden encontrarse en: <http://technet.microsoft.com/es-ar/security/dd252948>.



Figura 2. En <http://technet.microsoft.com> podemos encontrar innumerables recursos para aumentar la seguridad de sistemas Microsoft.

CONSEJOS PARA SISTEMAS UNIX

Estos sistemas cuentan con una gran reputación en lo que a seguridad se refiere. Pero debemos tener en cuenta que la gran cantidad de distribuciones UNIX que existen hace que cada una se enfoque en distintos objetivos, por lo que no todas pueden poner tanto énfasis en la seguridad. Es por eso que, al seleccionar el sistema UNIX que vamos a utilizar, debemos tener muchas consideraciones en mente, como las prioridades

del proyecto, el soporte del fabricante, la compatibilidad de hardware, el software disponible, etc. Entre las versiones libres, podemos distinguir la seguridad de los sistemas BSD (FreeBSD, NetBSD y OpenBSD), así como también de las distribuciones GNU/Linux Debian y RedHat.

El siguiente enlace contiene una excelente comparativa entre los sistemas operativos libres (excluye las versiones de UNIX propietarias, como HP-UX e IBM AIX):

http://es.wikipedia.org/wiki/Anexo:Comparación_de_los_sistemas_operativos_libres_y_de_código_abierto



Figura 3. En www.linuxsecurity.com podemos encontrar varios recursos acerca de la seguridad en sistemas operativos GNU/Linux.

Ya que estos sistemas nos permiten (y nos llevan a) ser minimalistas e instalar solo lo necesario para que cumplan sus funciones, debemos planear adecuadamente qué componentes instalar y cómo configurarlos. Además, todas las versiones serias cuentan con una guía de seguridad donde se recomienda cómo realizar la configuración.

HARDENING

El proceso conocido como hardening involucra varias tareas que buscan aumentar la seguridad de un sistema. Siempre debemos realizar dicho proceso al instalar un nuevo sistema o dispositivo. Cada sistema cuenta con sus mejores prácticas y guías que detallan cómo realizarlo adecuadamente y aprovechando todas las características de seguridad

Figura 4. En la consola de administración de servicios de Windows, podemos configurar varios parámetros para cada uno de los servicios.

Nombre	Descripción	Estado	Tipo de inicio	Iniciar sesión como
Acceso a dispositivo de interfaz humana	Habilita el...	Deshabilitado	Sistema local	
Actualizaciones automáticas	Habilita la d...	Deshabilitado	Sistema local	
Adaptador de rendimiento de WinM	Proporcion...	Manual	Sistema local	
Administración de aplicaciones	Ofrece ser...	Manual	Sistema local	
Administrador de conexión automática	Crea una c...	Manual	Sistema local	
Administrador de conexión de acceso...	...	Iniciado	Manual	Sistema local
Administrador de cuentas de seguridad	Almacena l...	Iniciado	Automático	Sistema local
Administrador de discos lógicos	Detecta y s...	Iniciado	Automático	Sistema local
Administrador de sesión de Ayuda de...	Administra...	Manual	Sistema local	
Adquisición de imágenes de Windows...	Proporcion...	Iniciado	Automático	Sistema local
Almacenamiento protegido	Ofrece alm...	Iniciado	Automático	Sistema local
Aplicación del sistema COM+	Administra l...	Manual	Sistema local	
Audíof de Windows	Administra...	Iniciado	Automático	Sistema local
Ayuda de NetBIOS sobre TCP/IP	Habilita la c...	Iniciado	Automático	Sistema local
Ayuda y soporte técnico	Habilita la c...	Iniciado	Automático	Sistema local
Centro de seguridad	Supervisa l...	Deshabilitado	Sistema local	
Cliente de seguimiento de vínculos d...	Monitoreo v...	Iniciado	Automático	Sistema local
Cliente DHCP	Administra l...	Iniciado	Automático	Sistema local
Cliente DNS	Resuelve y...	Iniciado	Automático	Servicio de red
Cliente Web	Habilita la...	Iniciado	Automático	Sistema local
Cola de impresión	Carga archi...	Iniciado	Automático	Sistema local
Compatibilidad de cambio rápido de u...	Proporcion...	Iniciado	Manual	Sistema local
Conexiones de red	Administra...	Iniciado	Manual	Sistema local
Configuración inalámbrica rápida	Proporcion...	Automático	Sistema local	
Coordinador de transacciones distrib...	Coordina la...	Manual	Servicio de red	
DDE de red	Ofrece tra...	Deshabilitado	Sistema local	
Detección de hardware shell	Proporcion...	Iniciado	Automático	Sistema local
DNSM de DOE de red	Administra...	Deshabilitado	Sistema local	
Redes de seguridad de acceso remoto	Ofrece ser...	Deshabilitado	Sistema local	

RECOMENDADOS

En el caso de los sistemas UNIX, podemos basar nuestro proceso de hardening en la lista de recomendaciones publicada por el **AusCERT**, que puede consultarse en www.auscert.org.au/5816. Allí se consideran varios aspectos, tanto de los sistemas operativos UNIX en general, como de métodos para implementar las medidas en sistemas específicos.

disponibles. Sin entrar en detalles acerca de cada uno, podemos decir que el hardening se basa en las siguientes tareas:

Minimizar la cantidad de servicios utilizados: la mayoría de los sistemas operativos se instalan por defecto con una cantidad de servicios habilitados que no siempre vamos a necesitar. Por ejemplo, el enrutamiento de paquetes, las conexiones inalámbricas (incluyendo infrarrojos

y Bluetooth), los puertos USB, y cualquier otro servicio que no vayamos a usar. Obviamente, dependiendo de las funciones que va a cumplir cada sistema, tendremos que seleccionar qué servicios habilitar y cuáles no. Pero debemos habilitar siempre lo mínimo necesario.

Utilizar interfaces de gestión seguras: si vamos a habilitar las interfaces de gestión remota, solamente debemos utilizar las que funcionen de forma segura, encriptando el tráfico y utilizando una buena política de accesos. De ser posible, es recomendable filtrar qué dispositivos pueden utilizarse para administrar los sistemas en forma remota. Analizaremos más sobre este tema en el apartado **Administración remota**.

Mantener el sistema actualizado: todos los sistemas tienen errores, que suelen ser corregidos con el lanzamiento de parches y actualizaciones. Debemos implementarlos siempre que sea posible, no solo para solucionar fallas, sino también para aprovechar funcionalidades de seguridad que pueden habilitarse con las nuevas versiones de los sistemas. Analizaremos más acerca de este aspecto en el apartado **Gestión de parches**.

Utilizar una buena política de contraseñas: es de suma importancia que las contraseñas de acceso (tanto de usuarios como de administradores) estén obligadas a cumplir con una política que garantice la dificultad de realizar ataques de cracking sobre ellas.

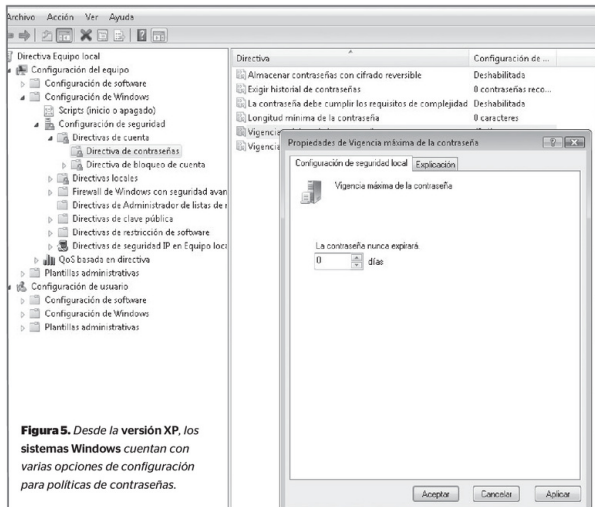
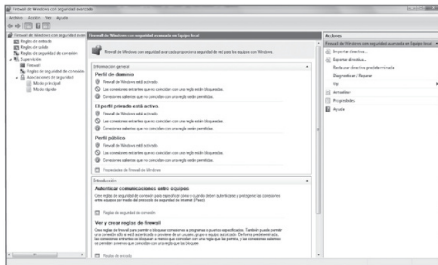


Figura 5. Desde la versión XP, los sistemas Windows cuentan con varias opciones de configuración para políticas de contraseñas.

Figura 6. El firewall de Windows 7 muestra que ha ido evolucionando con respecto a las versiones presentes en los sistemas anteriores.



Se recomienda, por lo menos, tener en cuenta los siguientes puntos:

- » Tener una longitud mínima (al menos 8 caracteres).
- » Realizar el cambio regular obligatorio (por ejemplo, cada 30 días).
- » No repetir claves (por ejemplo, ninguna de las últimas 12).
- » No utilizar palabras del diccionario.
- » Emplear mayúsculas, minúsculas y números.

Utilizar filtrado de conexiones (firewall): es recomendable implementar este tipo de filtros, por lo menos, en los servidores. Esto nos ayudará a limitar desde dónde y hacia dónde pueden establecerse las conexiones, lo cual nos permitirá

mantener a raya varios tipos de ataque. Trataremos más este tema en la sección **Firewalls**.

Separar las particiones de disco: cuando instalamos un servidor, debemos definir un esquema de particionamiento acorde a sus tareas específicas. Por lo menos, tenemos que establecer una partición para el sistema operativo y otra para los datos que se van a almacenar en él. Esto nos permitirá reinstalar el sistema rápidamente, sin perder la información de nuestra organización.

Utilizar autenticación centralizada: los servidores de autenticación centralizada (como **ActiveDirectory**, **OpenLDAP**, y otros) nos permitirán

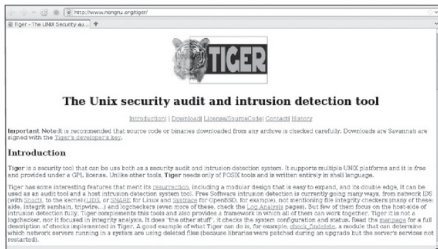


Figura 7. Tiger es un software para realizar varias comprobaciones de seguridad en los sistemas UNIX (www.nongnu.org/tiger).

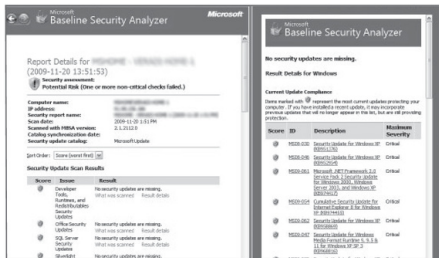


Figura 8. MBSA es una herramienta que nos permite analizar rápidamente la seguridad de los productos Microsoft. La podemos encontrar en la dirección www.microsoft.com/mbsa.

centralizar nuestra base de datos de usuarios e implementar políticas de contraseñas de una forma sencilla. Hablaremos sobre este tema con más detalle en la sección **Servidores de autenticación**.

Almacenar los registros de forma segura: los logs o registros de nuestros sistemas deben ser almacenados de forma segura y en un servidor remoto. De esta forma, podremos realizar varios análisis para determinar el estado de nuestra infraestructura y los sucesos relacionados con ella. Evaluaremos este aspecto en la sección **Análisis de logs**.

Crear copias de respaldo regularmente: como todo dato puede sufrir daños totales o parciales, es necesario implementar una política de copias de seguridad, y las herramientas adecuadas para llevarla a cabo. Profundizaremos en este tema en la sección **Backups**.

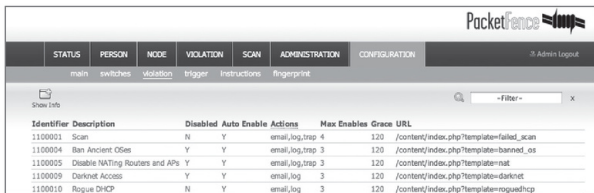
La nueva medida de seguridad que más se busca implementar en las infraestructuras es el control de dispositivos USB

(Fuente: Securosis Data Security Survey 2010)

EN LA PRÁCTICA PROFESIONAL

En las organizaciones, el proceso de hardening debe estar perfectamente documentado y estandarizado para que a cada dispositivo se le apliquen las mismas medidas de seguridad. Esto es importante porque cada medida de seguridad que implementemos podría no solo tener resultados positivos, sino también producir un mal funcionamiento en los sistemas y las aplicaciones relacionadas. Además, es preciso tener mucho cuidado al modificar las políticas de hardening que implementamos, verificando que cada cambio funcione de la forma en la que esperamos. Si es posible, tenemos que utilizar equipos de prueba. Por último, es importante prestar atención a las fuentes de documentación en las que nos basamos para realizar cambios. Es muy habitual encontrar "trucos ocultos" en algunos sitios web, que no hacen más que provocar un comportamiento extraño en nuestros sistemas o, lo que es peor, comportamientos que podrían parecer correctos, pero que no funcionan de manera adecuada. Este tipo de cambios deben ser probados antes de ponerlos en producción.





Identifier	Description	Disabled	Auto Enable	Actions	Max Enables	Grace	URL
1100001	Scan	N	Y	email_log,trap	4	120	/content/index.php?template=failed_scan
1100004	Ban Ancient OSes	Y	Y	email_log,trap	3	120	/content/index.php?template=banned_os
1100005	Disable NATing Routers and APs	Y	Y	email_log,trap	3	120	/content/index.php?template=nat
1100009	Darknet Access	Y	Y	email_log	3	120	/content/index.php?template=darknet
1100010	Rogue DHCP	N	Y	email_log	3	120	/content/index.php?template=roguedhcp

Figura 9. Packetfence es un software de código abierto que nos permite implementar NAC en nuestra red (www.packetfence.org).

MUST KNOW

Así como en el caso de la tecnología NIDS, la implementación de un sistema NAC es un proceso complejo, pero que puede ayudarnos a aumentar en gran medida la seguridad de nuestra infraestructura. Pero, a diferencia de los sistemas NIDS, la tecnología NAC está formada por varios componentes distintos, y debemos tener ciertas consideraciones con este tipo de proyectos:

Caídas de servicio: Estos sistemas podrían denegar el acceso a la red a dispositivos que deberían acceder normalmente.

Cambios necesarios: Es muy habitual que sea necesario realizar modificaciones en la infraestructura para implementar estas tecnologías. Debemos analizar cuidadosamente el costo que podrían llegar a tener estos cambios.

Alineamiento a futuro: Es preciso considerar que estas tecnologías nos permitirán evolucionar nuestra infraestructura, pero también, restringirán el modo en que esta puede hacerlo. Debemos considerar si el sistema NAC seleccionado nos permitirá crecer de acuerdo con nuestros planes.

NETWORK ACCESS CONTROL

NAC es una tecnología relativamente nueva, que pretende unificar tecnologías como anti-malware, prevención de intrusos y análisis de vulnerabilidades. Esto nos permite implementar varios controles sobre los dispositivos que están conectados a la red, tanto de preadmisión como de postadmisión, para decidir qué dispositivos pueden conectarse y a qué recursos de red pueden acceder.

El 34% de las empresas utiliza alguna solución de Network Access Control

(Fuente: CSI Computer Crime and Security Survey)

TECNOLOGÍA NAC

Esta tecnología se encuentra en constante evolución, y es implementada de diversas formas por varios fabricantes, que agregan diferentes funcionalidades a cada uno de sus productos. En los sistemas Microsoft Windows, encontramos una implementación llamada **Network Access Protection (NAP)**, que apareció en los sistemas Windows Server 2008. Por su parte, **Cisco Systems** desarrolló una denominada **Network Admission Control**.

En la mayoría de los casos, el funcionamiento de esta tecnología se logra a través de un

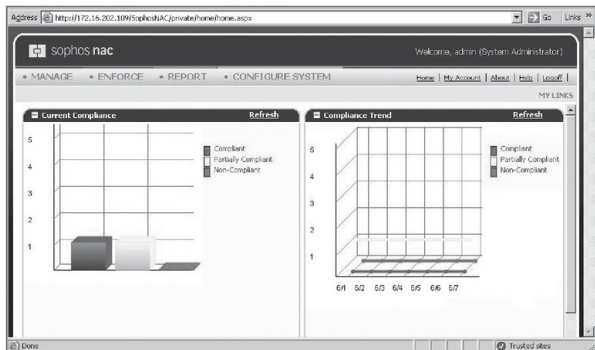


Figura 10. En la imagen podemos ver la solución de NAC ofrecida por el fabricante Sophos (www.sophos.com).

trabajo conjunto entre los servicios DHCP, DNS y los dispositivos de telecomunicaciones. Esto permite ubicar los dispositivos que no cumplen con la política de seguridad en una red de cuarentena, y remediar su situación instalando el software antimalware necesario e implementando las configuraciones requeridas por el administrador de la red. Con la nueva tendencia de los dispositivos móviles, como teléfonos inteligentes y computadoras portátiles, es muy común que los equipos que se conectan a nuestra infraestructura vengan de haberse conectado a varias redes, que pueden haberlos infectado. Por otra parte, este tipo de equipos requiere más control por parte de los usuarios, por lo que se les permite modificar cierto tipo de configuraciones, que podrían llegar a representar riesgos para la seguridad. Es por eso que estas tecnologías son la nueva tendencia en cuanto a seguridad corporativa, porque nos permiten minimizar los peligros a los cuales nos exponen las modernas formas de trabajo. Pero recordemos que son solamente

un componente de lo que debe ser nuestra estrategia de defensa en capas.

MALWARE

El **malware** es todo aquel software desarrollado con el objetivo de producir algún mal en el sistema sin el consentimiento de su propietario. Esta es una descripción muy general, que engloba a una gran cantidad de subtipos de software. Entre los más importantes podemos encontrar **virus, gusanos, rootkits, troyanos, spyware y keyloggers**. En particular, la mayoría del malware desarrollado busca atacar sistemas operativos Windows.

En 2010, Symantec encontró más de 286 millones de variantes únicas de malware

(Fuente: Symantec Internet Security Threat Report Trends for 2010)

El 64% de las empresas ha experimentado problemas de infección de malware

(Fuente: CSI Survey 2009)

La tecnología de seguridad más utilizada es el software antimalware, mientras que la menos usada es el control de acceso por biometría

(Fuente: CSI Computer Crime and Security Survey)

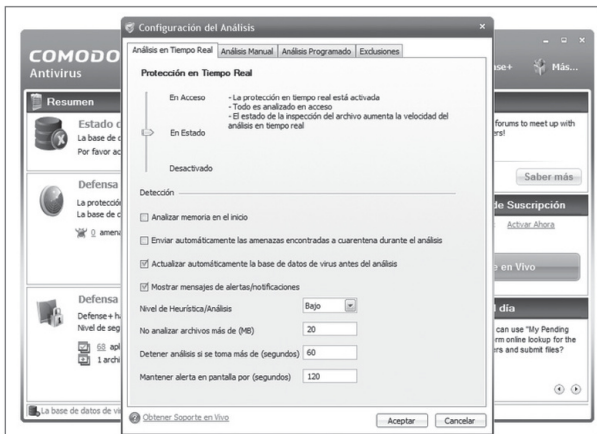
Figura 11. La empresa Comodo ofrece software gratuito para la protección contra malware (www.comodo.com).

RECOMENDADOS

A continuación, presentamos una lista con algunos de los fabricantes de software antimalware que ofrecen versiones gratuitas de sus productos: **Avast:** www.avast.com, **AVG:** www.avg.com, **Avira:** www.avira.com, **Fortinet:** www.fortclient.com y **Microsoft:** www.microsoft.com/security_essentials. Todos cuentan con versiones pagas de sus productos, que incluyen más funcionalidades.

En caso de que nuestra organización cuente con pocos dispositivos, podemos optar por instalar alguna de las soluciones gratuitas que se ofrecen en el mercado.

La mayoría provee capacidades de detección básicas, y no cuenta con la posibilidad de gestionarse en forma remota, aunque esto es algo que no nos preocupa si debemos



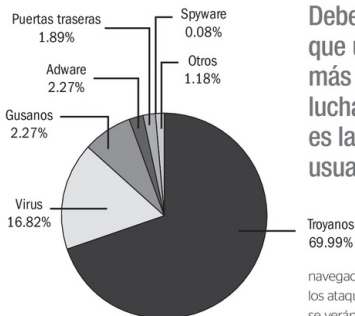


Figura 12. El gráfico muestra estadísticas sobre la clase de malware que se encuentra en Internet. La mayoría de ellos son troyanos.

proteger una pequeña cantidad de servidores y estaciones de trabajo.

Si nuestra organización cuenta con un gran número de dispositivos, debemos elegir una solución antimalware paga. En este caso, deberemos evaluar con mucho cuidado tanto las capacidades de detección, como el soporte y la interfaz de gestión centralizada que provee el fabricante. Estos tres factores son fundamentales al momento de seleccionar una solución de este tipo.

MUST KNOW

Además del software antimalware, existen otras medidas que podemos tomar para reducir el riesgo de infecciones. Por ejemplo, podemos implementar filtros de navegación web que bloqueen el acceso a sitios sospechosos. Mucho del malware existente se aloja en sitios de descargas gratuitas, pornografía, juegos online y otros similares.

Debemos tener en cuenta que una de las medidas más importantes para luchar contra el malware es la capacitación de los usuarios

Si ellos entienden que no deben ejecutar programas en los cuales no confíen, y que deben evitar la navegación por sitios web de dudosa reputación, los ataques por malware que sufrirá la empresa se verán disminuidos en gran medida.

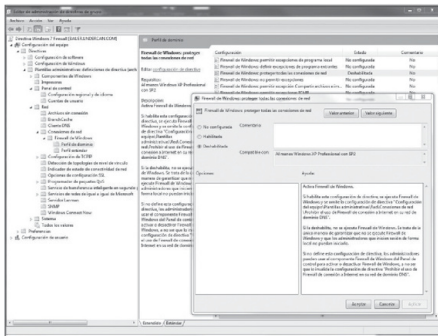
PROTECCIÓN EN CAPAS

Como analizamos en capítulos anteriores, el concepto de “defensa en profundidad” nos permite aumentar enormemente la seguridad de nuestros sistemas al implementar varias capas de defensa. En el caso del malware, esto puede llevarse a la práctica implementando varios controles en diferentes puntos de la red. Por ejemplo, podemos contar con:

- » Un dispositivo UTM que se encargue de analizar todo el tráfico que entra y sale de la conexión a Internet.
- » Un software antimalware en el servidor de archivos, que se ocupe de analizar todos los archivos alojados en él.
- » Un software antimalware en cada estación de trabajo.

Con estas tres capas de protección, correctamente administradas y actualizadas, se vuelve casi imposible que un software malicioso consiga ingresar en nuestra infraestructura. También debemos tener en cuenta que, si bien cada una de estas capas es importante, pueden

Figura 13. Aquí vemos cómo podemos configurar el firewall de Windows a través de Group Policies

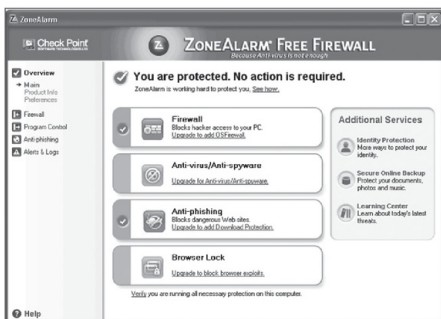


darse casos particulares en los que una sola tenga que hacer todo el trabajo. Por ejemplo, los virus que se alojan en un pendrive USB podrían ser detectados únicamente por el sistema antimalware de la estación de trabajo correspondiente. Por esta razón, es de vital importancia que cada una de las medidas de seguridad se encuentre en perfecto estado.

FIREWALLS

Actualmente, todos los sistemas operativos cuentan con sistemas de firewall, ya sea para servidores o para estaciones de trabajo. Tanto Windows Firewall (sistemas Windows), como IPTables (sistemas GNU/Linux) y PF (sistemas OpenBSD) son excelentes herramientas para

Figura 14. ZoneAlarm (www.zonealarm.com) es una excelente alternativa al firewall de Windows, que cuenta con una gran cantidad de características y es desarrollado por la famosa empresa de seguridad CheckPoint.



bloquear los puertos de nuestros sistemas a los que se puede acceder desde la red. En el caso de las plataformas Microsoft, podemos encontrar varias soluciones que intentan reemplazar al firewall incluido por defecto. En este caso, deberemos analizar qué ventajas y desventajas podría traernos implementarlas.

En los sistemas Windows, es posible realizar excelentes configuraciones a través de Active Directory, para mantener un estándar de puertos permitidos. Con esto nos aseguramos de bloquear algunos de los ataques más comunes realizando un esfuerzo mínimo.

El 50% de las empresas utiliza firewalls en sus servidores

(Fuente: CSI Computer Crime and Security Survey)

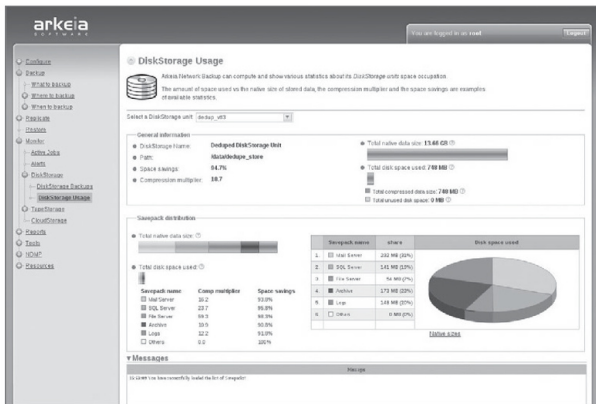
Debemos considerar la implementación de firewalls en las estaciones de trabajo como medi-

da de seguridad opcional, y analizar cuánto trabajo puede llevarnos mantener las reglas de filtrado de cada sistema, con respecto al beneficio de seguridad que nos representa. En la mayoría de los casos, deberemos optar por implementar una misma configuración para todas las estaciones de trabajo, con el fin de simplificar la gestión de reglas, aunque esto haga que nuestra configuración diste de ser perfecta.

Cuando nos referimos a estaciones de trabajo, generalmente no necesitamos que haya puertos abiertos a la espera de conexiones. Por lo tanto, podemos optar por cerrar todos los puertos, salvo los de administración remota.

En el caso de los servidores, debemos permitir únicamente las conexiones a los puertos de servicio, y solo desde los equipos que tienen motivo para conectarse.

Figura 15. El fabricante Arkeia cuenta con una gran cantidad de productos para el resguardo y la recuperación de datos (www.arkela.com).



BACKUPS

La mayoría de nuestros servidores (por no decir todos) tendrán alguna información que debería ser resguardada por si algo malo llegara a suceder. Y, cuando hablamos de algo malo, debemos considerar varias posibilidades, como fallas de discos, errores de usuario, ataques de malware, y otras acciones. Es por eso que la realización de copias de seguridad es una tarea prácticamente obligatoria en todos los casos. Solamente debemos pensar en la cantidad de datos por respaldar, la frecuencia de respaldo y el tiempo durante el cual vamos a almacenar las copias antes de eliminarlas.

Tanto si vamos a realizar copias de bases de datos, como de configuraciones, correos electrónicos u otros archivos, el uso de herramientas específicas nos simplificará la tarea de manera notable. Por esta razón, una de nuestras primeras decisiones cuando pensamos en respaldar los datos es seleccionar cómo lo haremos. Para esto, podemos optar por herramientas pequeñas, diferentes para cada sistema operativo; o por herramientas grandes, que se adaptan a cualquier entorno. Esta es una decisión que depende más de gustos que de necesidades.

El 47% de las empresas nunca realiza copias de seguridad de sus datos

(Fuente: Symantec 2010 SMB Information Protection Survey)

HERRAMIENTAS BASADAS EN AGENTES

Muchas herramientas del mercado que están basadas en la arquitectura cliente/servidor utilizan agentes instalados en cada uno de

los dispositivos de los cuales vamos a hacer copias de seguridad. Esto suele darles más control sobre los parámetros que se van a configurar, y permite que el agente realice tareas como compresión y encriptación de datos. En estos casos, son los agentes los que se conectan con el servidor principal para efectuar la transferencia de datos.

HERRAMIENTAS SIN AGENTES

Existen otras herramientas en las que el servidor realiza las conexiones cuando se van a generar los respaldos. Estas conexiones, por lo general, se hacen a través de interfaces de administración, como SSH, RPC o SNMP. Estas herramientas suelen ser menos flexibles, pero no están limitadas a los sistemas operativos para los cuales se haya desarrollado un agente.

SCRIPTS PERSONALIZADOS

Los grandes aliados de todo administrador de sistemas son los scripts personalizados que realizan tareas puntuales; por ejemplo, hacer una conexión a través de SSH, crear un archivo comprimido con todos los datos que se necesita respaldar, encriptarlo y transferirlo a través del protocolo FTP a otro servidor. Sin dudas, pode-

RECOMENDADOS

En la seguridad en redes tradicionales, se utiliza el bloqueo de puertos no válidos para protección, pero en aplicaciones web es necesaria la exposición del puerto 80 (HTTP), por lo que dispositivos como firewalls e IDS deben permitirlo y analizarlo internamente a fin de evitar ataques.

RECOMENDADOS

Algunas de las mejores herramientas para clonar discos, que cuentan con una gran cantidad de características, son: **Norton Ghost**, herramienta comercial (www.ghost.com); **Clonezilla**, de código abierto (www.clonezilla.org); y **MondoRescue**, de código abierto (www.mondorescue.org). Para consultar una lista más detallada: http://en.wikipedia.org/wiki/List_of_disk_cloning_software

mos sacar gran provecho de la implementación de este tipo de herramientas, que son pequeñas pero muy potentes.

Por ejemplo, con el código que se presenta a continuación, podemos, desde GNU/Linux, realizar una copia de las bases de datos MySQL de cualquiera de nuestros servidores:

```
#!/bin/bash
USER=usuario
PASS=clave

for db in `echo "show databases" | mysql
-u$USER -p$PASS | grep -v ^mysql$ | grep -v
^Database$`;
do
mysqldump --add-drop-table --routines -u
$USER -p $PASS ${db}> ${db}.sql;
done
```

RECUPERACIÓN COMPLETA

Existen herramientas desarrolladas con el objetivo de recuperar un sistema completamente, es decir, tanto el sistema operativo como los datos y las configuraciones. Esto se logra creando una imagen del contenido de los discos de almacenamiento. Este tipo de herramientas suele llamarse de "clonado de discos" o de "recuperación de

desastres", porque, en general, se utiliza en última instancia, cuando todo el sistema está inoperable. También son alternativas que pueden usarse para realizar instalaciones masivas, tanto de estaciones de trabajo como de servidores. Es un excelente recurso clonar discos para instalar automáticamente estaciones de trabajo preconfiguradas de forma segura.

AUTENTICACIÓN MULTIFACTOR

Para las conexiones a servicios críticos, podemos utilizar lo que se conoce como **autenticación multifactor**. En este caso, le solicitamos al usuario que se identifique no solo con una contraseña, sino también con algo que tiene en su poder, como una llave USB. Este es un concepto muy relacionado con el de **defensa en profundidad**, en el cual implementamos varias medidas de seguridad para proteger nuestros activos de información.

El 36% de las empresas utiliza alguna solución de SmartCards o tokens

(Fuente: CSI Computer Crime and Security Survey)

A continuación, analizaremos algunos de los factores de autenticación más utilizados.

TOKENS O SMART CARDS

Estos dispositivos electrónicos, básicamente, presentan una clave adicional que se genera en forma dinámica y aleatoria, y permite demostrar que el usuario se encuentra en posesión del dispositivo al momento de ingresar sus credenciales. Existen varios tipos de métodos para lograr este fin, pero, en principio, todos cumplen con la misma función.



Figura 16. Podemos ver uno de los tokens SecurID, desarrollados por RSA, que muestran ejemplos de los valores aleatorios generados.

TOKENS VIRTUALES

Los tokens virtuales buscan ser una alternativa más económica que los tradicionales, al recurrir a un dispositivo que el usuario ya posee. Esto suele lograrse con la instalación de un software en una laptop o teléfono celular del usuario, que cumple con funciones similares a las de un token tradicional. Si bien puede discutirse que el nivel de seguridad en este caso es inferior al de los tokens tradicionales o smart cards, estos son una excelente alternativa para aquellos casos en que nuestros recursos económicos son escasos.

Figura 17. Mobile-OTP que permite a los teléfonos celulares trabajar como dispositivos de token virtual (<http://motp.sourceforge.net>).

TARJETAS DE COORDENADAS

Una opción aún más económica se logra por medio de tarjetas que tienen una serie de filas y columnas, en las que cada combinación de fila/columna representa un código único. Al momento de autenticar al usuario, se le solicita a este que ingrese el valor, por ejemplo, de "Fila A - Columna 10".

La principal ventaja de este método es que las tarjetas pueden ser generadas automáticamente por un servidor, y distribuidas por medios electrónicos seguros (como un correo electrónico cifrado). Esto resulta en un costo prácticamente nulo.

Aunque debemos considerar que es el método

The screenshot shows the homepage of the Mobile-OTP project. At the top, the browser address bar displays 'http://motp.sourceforge.net/'. The page features a logo on the left showing a mobile phone with 'Mobile-OTP' text, and a central heading 'Mobile One Time Passwords' followed by 'Mobile-OTP' and 'strong, two-factor authentication with mobile phones'. A 'SOURCEFORGE.NET' logo is on the right. Below this, a list of news items is provided, including updates for Windows Phone 7, Linux, and various mobile devices. At the bottom, there is a link to 'Click for older news'.

Mobile One Time Passwords

Mobile-OTP

strong, two-factor authentication with mobile phones

Standard phone and BlackBerry (J2ME) (Phone Google Android Windows Phone 7 PalmOS webOS Meevo Openmoko Universal Web App)

first update of this site: June 5th, 2011

News

- (2011-05-02) motp7 by Steven Brunner is a new Mobile-OTP client for Windows Phone 7 (see [Links](#) section)
- (2011-05-04) Web-based, universal Mobile-OTP (also client that runs on any Internet device with Javascript) (see [Add-Ons](#) section)
- (2011-05-02) Swiss online payment provider SwiKey SA implements Mobile-OTP (see [Links](#) section)
- (2011-05-16) Eddi donated a server side alternative to openssl sh in Python (see [Add-Ons](#) section)
- (2011-03-31) SQL to authenticate users with PostgreSQL, in [Add-Ons](#) section
- (2011-03-27) Two more Mobile-OTP clients for Linux and Mac OS X (see [Links](#) section)
- (2011-02-04) Mobile-OTP client for Meevo (Palm OS) (see [Links](#) section)
- (2011-02-04) RPMs for the PAM module, including script for user management (see [Add-Ons](#) section)
- (2011-01-23) Mobile-OTP implemented in Ruby (see [Links](#) section)
- (2011-01-15) Simon Langley submitted a bash version of the speedily an script (Downloads)

[Click for older news](#)

	A	B	C	D	E	F	G	H
1	212	635	253	432	198	236	149	325
2	113	228	339	446	555	662	774	888
3	212	635	253	432	198	236	149	325
4	953	565	113	228	339	446	555	662
5	212	635	253	432	198	236	149	325
6	953	565	113	228	339	446	555	662
7	212	635	253	432	198	236	149	325
8	953	565	113	228	339	446	555	662
9	212	635	253	432	198	236	149	325
10	953	565	113	228	339	446	555	662

582 365 689

Figura 18. En la imagen podemos ver un ejemplo de una tarjeta de coordenadas utilizada por un banco para la autenticación de sus clientes.

más inseguro de todos, por varias fallas que podrían asociarse a esta técnica, podemos decir que es mucho mejor que utilizar autenticación simple. Junto con los tokens, es un método muy empleado en el sector bancario para realizar transferencias electrónicas de dinero.

Es mejor implementar una buena medida de seguridad económica, que no implementar una excelente medida de seguridad costosa

BIOMETRÍA

Esta tecnología se encarga de verificar la identidad del usuario comprobando factores que estén relacionados con la biología de la persona (de ahí el nombre, "biometría").

Algunas de las características más utilizadas son: escaneo de iris, escaneo de retina y escaneo de huellas dactilares.

Estos métodos tienen un alto porcentaje de fiabilidad, aunque poseen la desventaja de que los lectores tienen un costo relativamente elevado y no son muy portables, por lo que,

DEL EXPERTO

USUARIO Y CONTRASEÑA

Si hay un aspecto de la seguridad que se ha mantenido prácticamente sin modificaciones desde que empezaron a implementarse medidas de protección en los sistemas, Este es la autenticación por medio de usuario y contraseña. Los únicos cambios que sufrió con el correr de los años se han dado en la longitud y complejidad recomendada para las claves. Llegó el momento de empezar a implementar medidas de seguridad más avanzadas, debido a que la mayoría de las organizaciones emplea sistemas que procesan o almacenan su información crítica. Es por eso que se recomienda encarecidamente, por lo menos, realizar un análisis de la criticidad de los sistemas y, sobre esa base, estudiar la posibilidad de implementar tecnologías de autenticación multifactor. Debido a que el costo de estas tecnologías se ha reducido constantemente con el correr de los años, encarar este tipo de proyectos ya no supone efectuar una inversión económica tan importante como ocurría hasta hace algún tiempo.



Figura 19. Podemos ver un dispositivo que escanea huellas digitales y permite ingresar una clave numérica para controlar un acceso físico.



generalmente, se utilizan para accesos físicos y no tanto para accesos remotos.

SERVIDORES DE AUTENTICACIÓN

La administración de perfiles de usuario es otra de las tareas de importancia crítica para la seguridad informática, porque se encarga de definir quién, cómo y cuándo puede acceder a los sistemas. Es por eso que siempre debemos optimizar este tipo de tareas y las tecnologías que están relacionadas con ellas.

Al contar con un servidor que almacene la información de usuarios, grupos y perfiles, podemos determinar a qué servicios puede acceder una persona directamente modificando sus atributos.

Solo 10% de las empresas logra concentrar todo el proceso de autorización de usuarios en un único sistema

(Fuente: KPMG Information Security Survey)

Existen varias tecnologías que nos permiten implementar un servidor de autenticación centralizada, cada una, con sus respectivas ventajas y desventajas. Actualmente, las implementaciones más populares están basadas en el **protocolo LDAP**, que es una especie de base de datos que agrupa los registros en un formato de árbol. El producto más implementado actualmente es Active Directory (desarrollado por Microsoft), pero también hay otros, tanto comerciales como de código abierto. En el caso de los productos de código abierto, podemos destacar a **OpenLDAP**, **FreeIPA** y **Mandriva Directory Server**. **Active Directory** ofrece una integración muy fuerte con los clientes y servidores Windows, que nos permite implementar varias políticas de

RECOMENDADOS

La empresa WikID Systems ha desarrollado un software de servidor para autenticaciones multifactor, que cuenta con clientes para Windows, Mac, Linux, Blackberry, Palm, Windows Mobile y J2ME. Tiene una versión de código abierto y otra comercial, que ofrece una mayor cantidad de funcionalidades (www.wikidssystems.com).

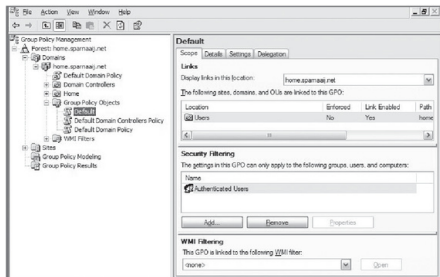


Figura 20. Las Group Policies de Active Directory nos permiten definir múltiples opciones de seguridad para nuestros equipos Windows.

seguridad y plantillas de configuraciones. Esto hace que, desde un único lugar, podamos implementar configuraciones, establecer políticas y distribuir software.

Los servidores de autenticación nos permiten centralizar no solamente las credenciales de acceso para nuestras estaciones de trabajo y servidores, sino también los accesos de nuestros dispositivos de telecomunicaciones. En el caso de Active Directory, podemos habilitar el protocolo Radius utilizando los mismos datos de cuentas que se encuentran en la base de datos LDAP del producto. Todas las soluciones de autenticación centra-

lizada tienen la posibilidad de brindar varios métodos de autenticación.

La mayoría de los accesos no autorizados suceden a través de cuentas de acceso autorizadas. Si las mantenemos controladas, habremos dado un paso importante

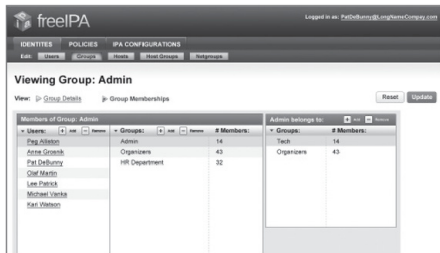
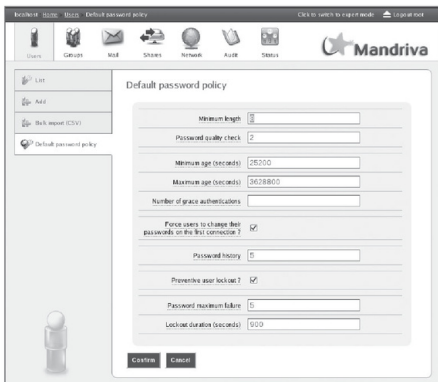


Figura 21. El proyecto FreeIPA ofrece una solución libre para la gestión de identidades. (<http://freelipa.org>)

Figura 22. MDS es un software que permite autenticar tanto equipos Microsoft Windows como equipos UNIX. (<http://mds.mandriva>).



ANÁLISIS DE LOGS

El almacenamiento y análisis de registros (o "logs") es una de las tareas más importantes en lo que a la seguridad informática se refiere. Muchas herramientas de seguridad están basadas en el análisis de este tipo de registros, y nos permiten conocer estadísticas y sucesos sospechosos, lo cual nos da la posibilidad de analizar tendencias y deducir comportamientos futuros. Además, debemos considerar que los atacantes siempre intentarán eliminar los registros en los sistemas en los que hayan podido penetrar, a fin de borrar las huellas del ataque. Otro aspecto importante del análisis de logs es que puede ser utilizado no solamente para conocer los eventos pasados, sino también para proyectar los eventos futuros. Este es un aspecto clave, porque un análisis detallado de los logs nos permitirá tomar decisiones acertadas acerca de qué medidas de seguridad implementar o reforzar. Es por este motivo que resulta fundamental contar con un servidor centralizado, en el cual podamos alma-

cenar todos los registros de nuestros sistemas. Una de las tantas diferencias que existen entre los sistemas operativos Windows y UNIX es el formato de logs utilizado en cada caso: "syslog" es el más empleado en UNIX (también utilizado en la mayoría de los dispositivos de telecomunicaciones), mientras que "EventLog" es el que emplean las plataformas Microsoft. Debemos tratar de unificar este tipo de logs, e implementar una herramienta que nos permita gestionar y analizar todos los datos en un único lugar.

MUST KNOW

Ya sea a través de herramientas complejas o de pequeños scripts realizados en algún lenguaje como Perl o Python, debemos implementar alguna metodología de análisis de logs. Esto nos permitirá simplificar nuestras tareas, realizar análisis en tiempo real, recibir notificaciones y contar con una mejor comprensión de nuestra infraestructura.

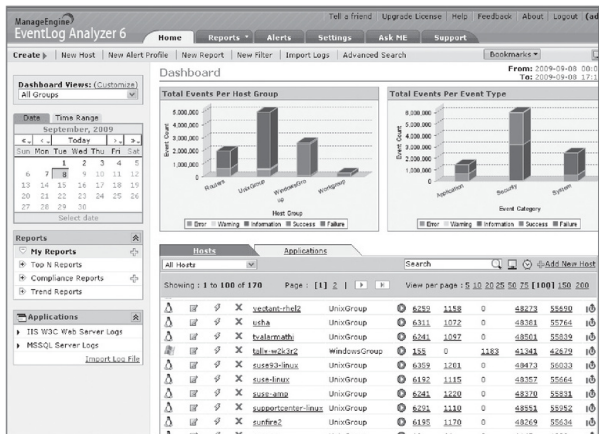


Figura 23. EventLog Analyzer, que nos permite centralizar los logs en formato tanto Syslog como EventLog (www.managenengine.com).

SERVIDORES CENTRALIZADOS

Para poder realizar un verdadero análisis de los logs de nuestros dispositivos, es necesario que estos se encuentren centralizados en un único lugar. Esto, además, nos permitirá hacer una correlación de los datos, de modo que podremos reaccionar no solo ante los eventos ocurridos en un sistema, sino también sobre la base de la relación que existe entre los eventos de varios sistemas. La correlación de eventos es de suma importancia si verdaderamente queremos tener un control sobre lo que sucede en nuestra infraestructura, porque no siempre podemos obtener toda la información necesaria de un único dispositivo. Por el contrario, a veces necesitamos

varias fuentes de información para comprender exactamente qué es lo que está sucediendo. Debemos prestar mucha atención a configurar correctamente el servidor central, para que los logs se almacenen como corresponda, no puedan ser modificados y se les haga una copia de seguridad en forma regular. También tenemos que considerar que el servidor de logs podría ser nuestro único recurso para analizar las características de un ataque o cualquier otro evento que haya impactado negativamente en la infraestructura. A continuación, explicamos algunos de los aspectos de seguridad que debemos considerar al implementar un servidor de logs centralizado:

» Los archivos de logs no pueden ser modificados, salvo para eliminarlos cuando haya pasado el tiempo de retención definido.

- » Los logs deben ser analizados automáticamente, para generar reportes de fácil comprensión.
- » Se debe implementar un sistema de alertas, que notifique a los administradores acerca de sucesos que requieran atención inmediata.

ADMINISTRACIÓN REMOTA

Las herramientas de administración remota son utilizadas, normalmente, para gestionar los servidores y otros dispositivos sin tener necesidad de acceder físicamente a ellos. Esta comodidad es

Figura 24. InterSect Alliance (www.intersectalliance.com) desarrolla herramientas cuyo objetivo es centralizar y analizar los logs de varios tipos.

casi necesaria, pero debemos tomar los recaudos de seguridad apropiados al implementar estas tecnologías. Gracias a este tipo de herramientas, podemos tanto simplificar nuestras tareas y optimizar nuestro trabajo, como abrir grandes vulnerabilidades en los sistemas. Es por eso que debemos planificar correctamente la implementación de herramientas y protocolos de gestión remota. Algunas de las consideraciones para tener en cuenta son comunes para todas ellas, como buenas políticas de autenticación, encriptación de datos, etc. De ser posible, debemos seleccionar una misma herramienta de gestión para todos los dispositivos o, por lo menos, una herramienta para cada tipo de plataforma (por ejemplo, UNIX, Windows y Cisco).

File Edit View Go Bookmarks Tools Help

http://snareserver.intersectalliance.com/SNARE/ConfigChecking/SystemConfig/PIXConfig/SNARE.org

SNARE SNARE Enterprise Security Monitoring
(DEVELOPMENT SERVER MODE)

Log Out My Account

System Security Monitoring Application Auditing Network Event Analysis Configuration Checking Status and Statistics Share Agent Information SNARE Server Utilities

/Configuration /System Security /PIX/Router Config

Testing Configure Scheduled Tasks Access Control

Summary

This objective allows you to interrogate the configuration of a CISCO IOS capable device, such as a PIX firewall, or a CISCO Router. The objective will attempt to connect to the device using the 'telnet' protocol, and display the current configuration. The current configuration will also be compared against an authorised 'Master', and changes will be highlighted.

This objective was regenerated on 29 August 2005 11:02:04

Regenerate Interactive

Original	New
Building configuration...	Building configuration...
: Saved	: Saved
:	:
PIX Version 6.1(2)	PIX Version 6.1(2)
nameif ethernet0 outside security0	nameif ethernet0 outside security0
nameif ethernet1 inside security100	nameif ethernet1 inside security100
nameif ethernet2 dmz security50	nameif ethernet2 dmz security50
enable password ***** encrypted	enable password ***** encrypted
passwd ***** encrypted	passwd ***** encrypted
access-list acl_out permit tcp any host outside_email eq www	access-list acl_out permit tcp any host outside_email eq www
	+ access-list acl_out permit tcp any host outside_email eq something
access-list acl_out permit tcp any host outside_email eq pop3	access-list acl_out permit tcp any host outside_email eq pop3
access-list 80 permit ip 192.168.100.0 255.255.255.0 10.0.3.0 255.255.255.0	access-list 80 permit ip 192.168.100.0 255.255.255.0 10.0.3.0 255.255.255.0
access-list 80 permit ip 192.168.100.0 255.255.255.0 10.0.4.0	



PORT KNOCKING

Se trata de un mecanismo para abrir puertos externamente en un firewall mediante una secuencia preestablecida de intentos de conexión a aquellos que están cerrados. Una vez que el firewall recibe una secuencia de conexión correcta, sus reglas son modificadas para permitir que el host que realizó los intentos se conecte a un puerto específico. Si bien la idea no ha sido puesta en práctica en una gran cantidad de organizaciones, representa una excelente opción cuando necesitamos dejar un acceso externo hacia nuestros sistemas para casos de emergencia, pero buscamos que dicho acceso esté cerrado la mayor parte del tiempo. Normalmente, se utiliza en conjunto con SSH, para

Figura 25. Splunk permite analizar varios tipos de datos, con el objetivo de saber todo lo que sucede en nuestra red. (www.splunk.com)

tener acceso a una línea de comandos del algún equipo de nuestra infraestructura. Es casi imposible que una persona que no conozca la secuencia correcta para abrir un determinado puerto consiga detectar el comportamiento de nuestros sistemas, de modo que es un método realmente seguro para un acceso remoto.

WMI

Windows Management Instrumentation es una serie de extensiones que permiten realizar

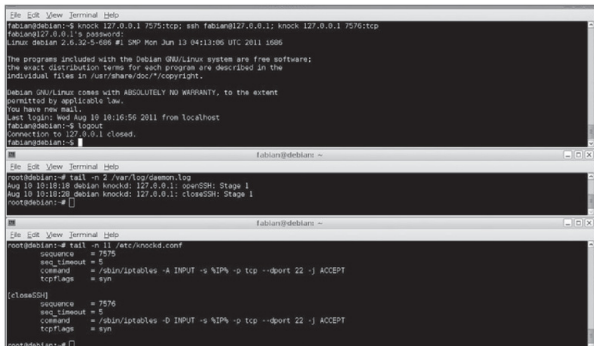
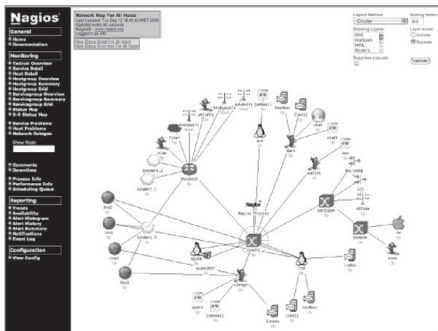


Figura 26. Vemos la utilización de knockd para implementar un solución de Port Knocking en sistemas Linux. (www.zeroflux.org/projects/knock)

la administración remota de sistemas Microsoft Windows. Está basado en los estándares abiertos WBEM y CIM, desarrollados por el

Distributed Management Task Force (DMTF). Utiliza la autenticación del propio sistema operativo, que suele ser por base de datos interna o por Active Directory, lo que nos permite simplificar la asignación de perfiles, y definir quién puede administrar los equipos y quién no. En el ejemplo que está a continuación, observa-

Figura 27. Algunos de los plugins para Nagios nos permiten agregar soporte para monitoreo a través de WMI. (<http://exchange.nagios.org/>)



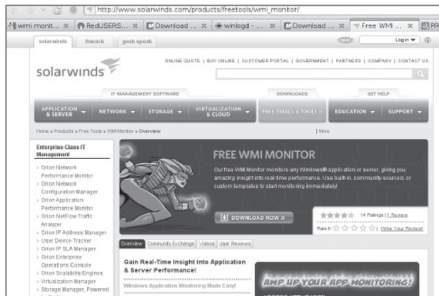
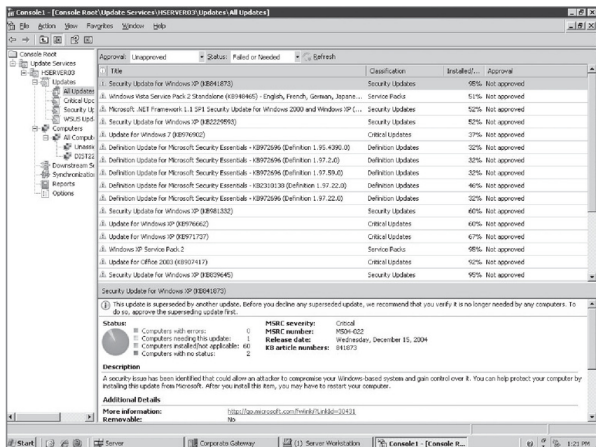


Figura 28. Solarwinds desarrolla herramientas para el monitoreo de redes, muchas de ellas, con soporte para WMI (www.solarwinds.com)

mos cómo puede utilizarse WMI a través del lenguaje C# para consultar el SSID de la red inalámbrica actualmente conectada:

Figura 29. MMC es la herramienta de los sistemas Windows destinada a la administración de usuarios, servicios y otros parámetros.



```

ManagementClass mc = new
ManagementClass("root\\WMI",
"MSNdis_80211_ServiceSetIdentifier", null);
ManagementObjectCollection moc = mc.
GetInstances();

foreach (ManagementObject mo in moc)
{
    string wlanCard = (string)
    mo["InstanceName"];
    bool active;
    if (!bool.TryParse((string)mo["Active"], out
    active))
    {
        active = false;
    }
    byte[] ssid = (byte[])mo["Ndis80211Ssid"];
}

```

RDP Y VNC

Remote Desktop Protocol y **Virtual Network Computing** son protocolos desarrollados para permitir el acceso remoto a los escritorios, tanto de estaciones de trabajo como de servidores. En ambos casos, existen versiones disponibles para

RECOMENDADOS

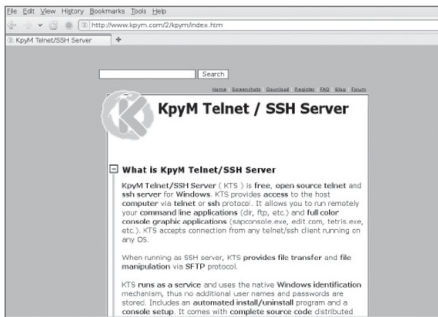
Una de las implementaciones más populares de código abierto del protocolo VNC para sistemas Windows es **UltraVNC**. Este software cuenta con muchas características interesantes, como autenticación por Active Directory, transferencia de archivos, encriptación de datos, y otras. El proyecto ha desarrollado tanto un cliente como un servidor (www.uvnc.com).

sistemas UNIX y Windows. Si vamos a utilizar este tipo de protocolos, debemos asegurarnos de configurarlos correctamente, para evitar posibles accesos no autorizados.

SSH

Como analizamos en el capítulo anterior, el protocolo SSH puede ser utilizado tanto para administrar servidores como para implementar conexiones del tipo VPN o crear túneles para aplicaciones específicas. Es particularmente popular en los sistemas del tipo UNIX.

Figura 30. KTS es un servidor de Telnet y SSH para los sistemas operativos Windows (www.kpym.com).



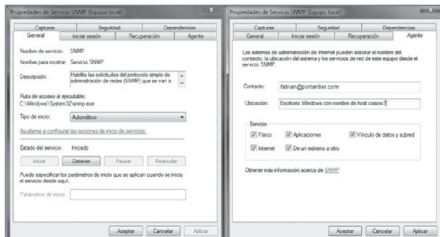


Figura 31. En Windows, podemos habilitar el componente de SNMP con la opción Agregar o quitar programas, del Panel de control.

SNMP

También vimos en el capítulo anterior que SNMP puede ser utilizado tanto para consultar como para modificar valores en los sistemas. Si bien su uso es más frecuente en dispositivos de telecomunicaciones, existen versiones para sistemas Microsoft Windows y UNIX.

WEBMIN

Este software nos permite contar con una **interfaz de gestión web (WUI)** para nuestros sistemas UNIX. Es un proyecto de código abierto que lleva varios años en el mercado y tiene módulos para gestionar infinidad de aspectos del sistema

operativo, tanto para las configuraciones básicas de usuarios, almacenamiento, red y firewall, como para los servicios de DNS, DHCP, SMTP y muchos otros. Su implementación puede simplificar de manera notable la gestión de los servidores, permite realizar tareas distribuidas entre varios equipos diferentes y define perfiles de acceso para cada uno de los usuarios. Por lo tanto, es un excelente complemento para otros accesos, como SSH.

DETECCIÓN DE INTRUSOS

Existen diversos tipos de software diseñados para prevenir intrusiones en hosts (**Host-based Intrusion Prevention Systems**, HIPS). Particularmente, hay ciertos factores para observar en

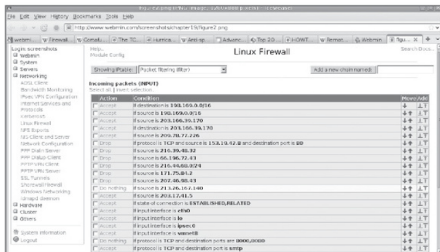
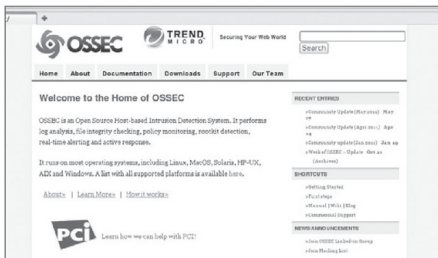


Figura 32. En el sitio web de Webmin podemos encontrar varios módulos para agregar funcionalidades (www.webmin.com).

Figura 33. OSSEC es un HIDS que funciona tanto en plataformas UNIX como en Microsoft Windows (www.ossec.net).



un sistema operativo, tendientes a detectar si hemos sido víctimas de una intrusión. Entre ellos, algunos de los más importantes son:

Integridad de archivos: se verifican el tamaño, los permisos, el hash y otros parámetros de cada uno de los archivos del sistema. En caso de encontrar cambios inesperados, estos son reportados.

Monitoreo de registros: se verifican constantemente los archivos de registro (logs), con el objetivo de detectar sucesos extraños o no deseados.

Registro de Windows: en el caso de las plataformas Microsoft, se verifican todas las claves de registro y se analizan los cambios realizados.

Puertos abiertos: se define una configuración que determina qué puertos deben estar abiertos. En caso de producirse cambios, estos son notificados. Cada herramienta particular puede tener características adicionales, pero todas, básicamente, apuntan a detectar comportamientos extraños o no deseados en el sistema operativo, y a reportarlos y/o bloquearlos.

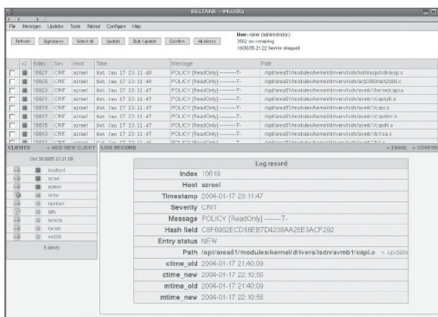


Figura 34. Samhain es uno de los mejores HIDS de código abierto disponibles para sistemas UNIX.

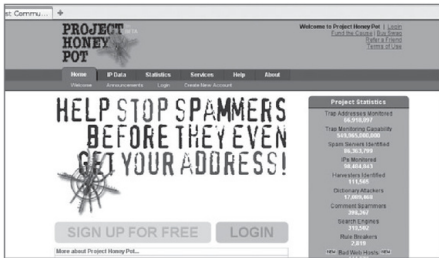


Figura 35. ProjectHoneyPot permite que cada dueño de un dominio pueda contribuir a detectar spammers.

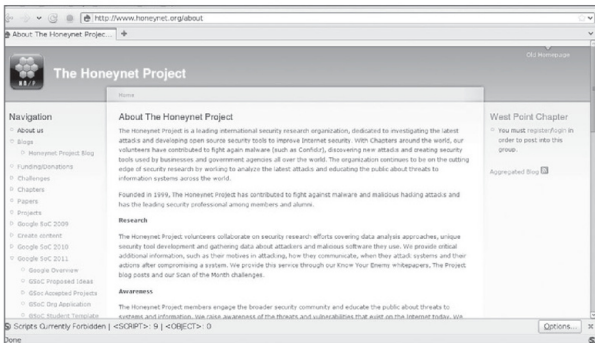
HONEYPOTS

Este tipo de sistemas busca implementar una especie de **trampa**, para atraer tanto a los atacantes como al malware que intente dispersarse automáticamente. La idea principal se basa en el concepto de que, si el sistema se encuentra exclusivamente dedicado a su función de honeypot, cualquier intento de conexión que se haga sobre él puede considerarse como **malintencionado**, porque ese dispositivo no cumple ninguna

función real para la organización.

Los honeypots suelen emular distintos sistemas operativos —Microsoft Windows, GNU/Linux, Cisco IOS, etcétera—, y aparentar el ofrecimiento de servicios vulnerables (como software

Figura 36. Honeynet investiga los últimos ataques y desarrolla herramientas de código abierto para aumentar la seguridad de los sistemas



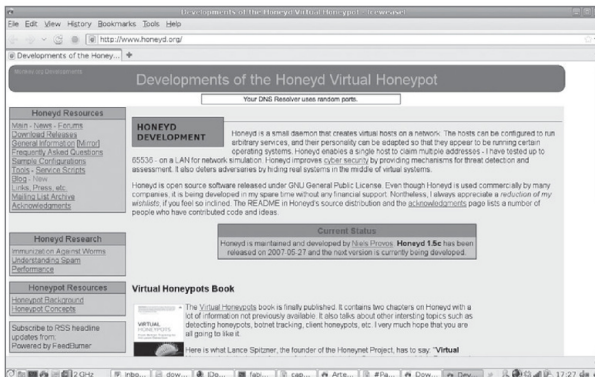


Figura 37. El proyecto Honeyd es uno de los honeypots de código abierto más desarrollados (<http://www.honeyd.org/>).

desactualizado o mal configurado), para atraer, en particular, a los atacantes que realizan escaneos de la red. Verdaderamente, ninguno de estos servicios es prestado, sino que se utilizan programas falsos que escuchan en los puertos correspondientes, y responden de manera igual o similar a los sistemas originales. De esta mane-

ra, los atacantes nunca tomarían control real del sistema honeypot. Además, suelen utilizarse técnicas para tomar automáticamente direcciones de red libres, y contestar a conexiones de red realizadas a direcciones que no están ocupadas por ningún sistema real.

“La implementación de este tipo de sistemas requiere analizar constantemente toda conexión que se realiza a ellos

RECOMENDADOS

Existen varias herramientas **HIPS** de código abierto, algunas disponibles para múltiples plataformas y con versiones pagas que brindan una mayor cantidad de funciones, como gestión centralizada. Algunas de las más reconocidas son: **Tripwire** (<http://sourceforge.net/projects/tripwire>), **OSSEC** (www.ossec.net) y **Samhain** (<http://www.la-samhna.de>).

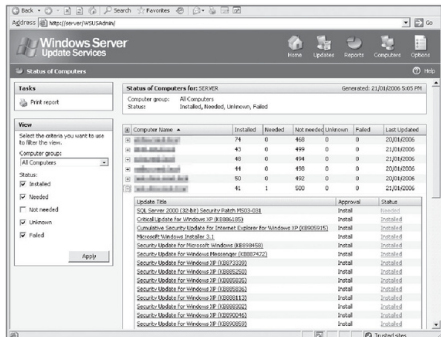


Figura 38. La plataforma WSUS, permite gestionar las actualizaciones de los productos desarrollados por Microsoft (www.microsoft.com).

Ya sea de forma automática (recomendada) o manual, debemos estar al tanto de los sistemas que envían tráfico a las direcciones de red tomadas por nuestro honeypot.

GESTIÓN DE PARCHES

Una de las tareas más importantes y críticas en cuanto a la administración de sistemas operativos es la gestión de los parches, que comprende tanto la selección, como la manera y el momento de aplicarlos. Este tipo de decisiones debe tomarse sobre la base de varios factores, como el propósito del sistema, su criticidad y las características del parche en cuestión.

El 65% de las empresas utiliza alguna solución de gestión de parches

(Fuente: CSI Computer Crime and Security Survey)

Como analizamos en capítulos anteriores, es de gran utilidad contar con sistemas dedicados exclusivamente a pruebas, para evitar el hecho de aplicar

un parche sin saber qué impacto puede tener en el funcionamiento de nuestro sistema de producción. Cada sistema operativo cuenta con sus herramientas propias para realizar la gestión de parches y actualizaciones. En el caso de Microsoft, disponemos de la plataforma WSUS (**Windows Server Update Services**), que es de uso gratuito y ofrece una gran cantidad de funciones, tendientes a satisfacer las necesidades de la mayoría de las empresas. En lo que se refiere a plataformas UNIX, cada distribución incluye sus herramientas particulares. Y siempre tenemos la opción de personalizar el comportamiento a través de scripts.

RECOMENDADOS

Existen honeypots desarrollados para emular exclusivamente un tipo particular de sistema, con el objetivo de atraer solo cierta clase de ataques o malware. Dos ejemplos son **Artemisa** (<http://artemisa.sourceforge.net>), que emula un sistema de voz sobre IP; y **SpamHole**, que emula un servidor de correo mal configurado (<http://sourceforge.net/projects/spamhole>).

Figura 39. Spacewalk permite administrar la configuración de los sistemas operativos basados en RedHat (<http://spacewalk.redhat.com>).

The screenshot displays the Spacewalk web interface. At the top, there's a navigation bar with links like 'Your RPM', 'Systems', 'Errata', 'Channels', 'Configuration', 'Schedule', 'Users', 'Save the Tools', 'Developer's Area', and 'Help'. Below this, the main content area is divided into several sections:

- Your Spacewalk**: A sidebar with links to 'Your RPM', 'Your Preferences', 'Local Preferences', 'Subscriptions', and 'Management'.
- Tools**: A list of actions including 'Search for Packages', 'Manage Entitlements and Subscriptions', 'Register Systems', 'Manage Activation Keys', 'Manage Kickstarts', 'Manage Configuration Files', and 'Configure Spacewalk'.
- Search Results**: A table showing search results for 'Systems'. It lists systems like 'dhcp-68-12.dev.example.com' and 'dhcp-69-08.dev.example.com' with their respective counts and links to view details.
- Most Critical Systems**: A table showing the most critical systems. It lists systems like 'YE_system_juMP_386_4AS' and 'herts' with their counts and links to view details.
- Recently Scheduled Actions**: A table showing recently scheduled actions. It lists actions like 'Package Install' and 'Package Update' with their counts and links to view details.
- Released Security Errata**: A table showing released security errata. It lists errata like 'RHSA-2008-0120' and 'RHSA-2008-0233' with their counts and links to view details.

MUST KNOW

Ya sea que tomemos la decisión de aplicar un determinado parche o no, siempre debemos estar al tanto del propósito que este tiene. Como ya mencionamos, es preciso tener un completo conocimiento acerca de cada uno de los cambios que elegimos aplicar o no aplicar en nuestros equipos. El error o el acierto estará en el porqué de la decisión, y no en la decisión en sí.

PARA PONER A PRUEBA

1. ¿Qué aspectos debemos tener en cuenta al elegir un sistema operativo?
2. ¿Qué es y por qué es importante el hardening de sistemas?
3. ¿Para qué sirve la autenticación multifactor?
4. ¿En qué casos puede ser beneficioso implementar port knocking?
5. ¿Cómo implementamos defensa en profundidad contra el malware?
6. ¿Qué es y para qué sirve un honeypot?

CAPÍTULO 6

NUEVAS TENDENCIAS

PARA APROVECHAR ESTE CAPÍTULO

- » **DESCARGAR** LOS DOCUMENTOS A LOS QUE SE HACE REFERENCIA DURANTE EL CAPÍTULO.
- » **CONSIDERAR** TODAS ESTAS TECNOLOGÍAS DENTRO DE NUESTROS PROYECTOS FUTUROS.
- » **IDENTIFICAR** LAS POSIBLES BRECHAS DE SEGURIDAD QUE PUEDEN ABRIR LAS NUEVAS TECNOLOGÍAS EN NUESTRA INFRAESTRUCTURA.

NUEVAS TENDENCIAS

En este capítulo aprenderemos a:

Objetivo 1 Reconocer los peligros de las tecnologías móviles.

Objetivo 2 Conocer, en profundidad, las consideraciones adecuadas para implementar tecnologías de virtualización.

Objetivo 3 Tener una visión acerca de las nuevas tendencias en tecnología y lo que implican para la seguridad.

Como ya hemos analizado durante los capítulos anteriores, la tecnología avanza constantemente, evoluciona a un ritmo acelerado. Por desgracia, los peligros que podemos encontrar, avanzan de la misma forma.

Podemos afirmar, sin temor a equivocarnos, que hace muchos años que no tenemos **tranquilidad** en el ambiente tecnológico. Es decir, prácticamente todos los años aparece un nuevo producto o tecnología que genera una revolución en nuestras vidas. Esto provoca cambios en la forma de trabajar, de pensar y de vivir, por lo que, a veces, la tecnología marca las tendencias, y a veces, tiene que evolucionar para seguirse el paso a sí misma. Particularmente, la seguridad informática se encuentra siempre un paso por detrás del resto de los aspectos tecnológicos, no por carecer de creatividad o de especialistas, sino porque su

propósito es reaccionar ante cualquier nuevo comportamiento que pudiera poner en peligro tanto a las personas como a las organizaciones que utilizan las nuevas tecnologías.



Nuestra misión:
que las personas y las organizaciones puedan aprovechar al máximo las nuevas tecnologías, teniendo cuidado de que se las utilice en forma segura

Esto hace que la profesión sea extremadamente emocionante, y le da una naturaleza de investigación constante, que pocas otras profesiones encuentran. En las páginas siguientes analizaremos cuáles son las nuevas tendencias, las

tecnologías emergentes, y cómo podemos implementarlas sin poner en riesgo la seguridad de la organización.

WEB 2.0

Este concepto no se refiere a una actualización de las tecnologías o protocolos, ni a un uso puntual de ellos, sino más bien a una nueva forma de desarrollo que tiene como objetivo poner a la Web en el centro de la escena para facilitar la posibilidad de compartir información, la interoperabilidad, el diseño centrado en el usuario y la colaboración. Esto dio nacimiento a las comunidades web, los servicios web, las aplicaciones web, las **redes sociales**, los **servicios de alojamiento de videos**, las **wikis**, los **blogs**, y otros servicios. Particularmente, algunas de las tecnologías más involucradas en la **Web 2.0** son **CSS**, **AJAX**, **RSS**/

ATOM, **XML** y **JSON**, entre otras. En esta "nueva Web", el usuario es el protagonista principal, que tiene la capacidad de publicar contenidos, conectarse con otras personas e interactuar con toda la infraestructura disponible, que antes se utilizaba solo para leer información.

Si bien el concepto de **Web 3.0** (principalmente, la Web semántica) está rondando hace varios años, podemos decir que el gran salto de paradigma fue dado por lo que sería su predecesor, en el cual encontramos una fuerte cantidad de nuevos beneficios y peligros.

REDES SOCIALES

Sin lugar a dudas, las redes sociales, como **Facebook**, **Twitter** y **GooglePlus**, son la nueva tecnología en expansión. Su misión: permitir que cualquier usuario genere contactos con otras

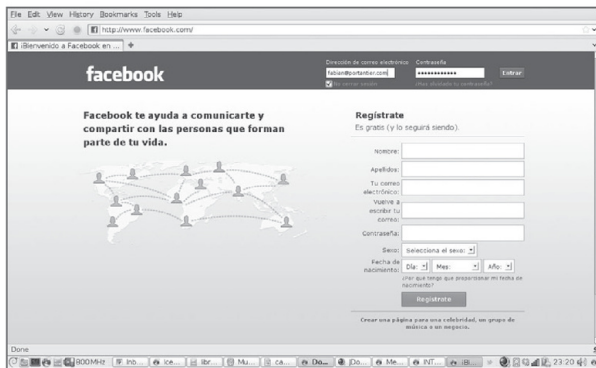


Figura 1. Facebook se ha convertido en la red social más popular, en 2011 contaba con más de 600 millones de usuarios, y se ha vuelto el objetivo de muchísimos ataques. En algunos de los cuales le provocaron grandes problemas de seguridad. Para obtener más información acerca de buenas prácticas de seguridad en su uso, podemos visitar www.facebook.com/safety.

personas y comparta información rápidamente, aunque también permiten la proliferación de malware, ataques y estafas.

Para una organización, antes era fácil bloquear los accesos a estos tipos de redes, que solamente se utilizaban para el ocio. En la actualidad, existen redes desarrolladas con fines laborales, como **LinkedIn**, que las mismas organizaciones emplean para reclutar personal o hacer otros contactos de negocios. También Facebook se está empezado a utilizar como medio de promoción para las empresas. Por estos motivos, ya es casi imposible bloquear este tipo de accesos, porque la publicidad web se encuentra dentro de los planes de toda organización actual. Pero debemos ser cuidadosos, y permitir el acceso a este tipo de redes solo a aquellas personas que verdaderamente lo necesitan.

Otra problemática que se genera en todas las organizaciones es que los usuarios pueden revelar información confidencial de la empresa a través de estas redes, aun cuando no están en la oficina, sino desde sus casas, usando sus computadoras personales.

Por lo tanto, es de vital importancia contar con un buen plan de capacitación, que haga entender a los usuarios los peligros potenciales a los que exponen a su organización al divulgar información privada.

MUST KNOW

Las casillas de correo electrónico de tipo web como Gmail o Hotmail no son analizadas por el antivirus residente a menos que descarguemos su contenido desde un cliente POP3 como Windows Mail. Sin embargo, estos servicios siempre cuentan con un antivirus online razonable. Podemos controlar su activación en las opciones del correo web.

GOOGLE HACKING

Con este término se conoce a las técnicas para recabar información de una organización a través de los buscadores de Internet, —particularmente, utilizando **Google**. Esto no es algo que puede catalogarse como un ataque en sí, pero sí puede ser de gran importancia para determinar el éxito o el fracaso de un atacante.

“Actualmente, los buscadores de Internet almacenan muchísima información acerca de los sitios web que analizan

Además, buscadores como Google ofrecen varias opciones de búsqueda para encontrar tipos de archivo específicos, buscar solo dentro de un dominio particular, y muchos otros parámetros. Para protegernos de las búsquedas de información sensible en nuestros servidores web, podemos enumerar las siguiente consideraciones:

1. No alojar información verdaderamente confidencial en los servidores web.
2. Prohibir el listado de directorios.
3. Utilizar el archivo estilo comando **.txt** para definir qué secciones de nuestro sitio web van a catalogar los robots de los buscadores, para más información, recomendamos visitar: **www.robotstxt.org**.
4. Proteger las secciones privadas de nuestro sitio web mediante contraseñas.

Si queremos que nuestro sitio web detalle qué partes no deben ser analizadas por los robots de los buscadores, podemos ubicar el archivo **robots.txt** en la raíz, con un contenido como el siguiente:

```
User-agent: *
Disallow: /administrator/
Disallow: /images/
Disallow: /includes/
Disallow: /templates/
Disallow: /tmp/
```

Pero debemos recordar que este tipo de configuraciones solo funciona si los robots respetan estos archivos. Los buscadores más famosos, como **Google, Yahoo!** y **Bing**, sí lo hacen. Como siempre, uno de los métodos más efectivos para protegernos, es verificar qué información relacionada con nuestra organización aparece en los buscadores web. Para esto, la forma más sencilla es ingresar en el sitio de algunos buscadores y realizar consultas a partir del nombre de nuestra empresa y de otros aspectos relacionados con ella, como teléfonos y direcciones de correo electrónico, entre otros.

MUST KNOW

Es de suma importancia que los usuarios tomen conciencia y entiendan que todo lo que se publica en los medios de Internet se vuelve automáticamente de dominio público. Más allá de que hayamos configurado opciones de privacidad en las redes sociales, actualmente, en Internet, el concepto de privacidad no existe.

PHISHING Y ROBO DE IDENTIDAD

Este concepto no es nuevo, pero ha evolucionado a la par de las nuevas tecnologías. Se trata, básicamente, de estafas que se realizan a partir de generar una falsa identidad, para que el usuario crea que está ante un ente de su confianza y, así, entregue información confidencial, como credenciales, números de cuentas bancarias, datos personales, y más. Si bien podemos encontrar que existen muchas tecnologías y técnicas

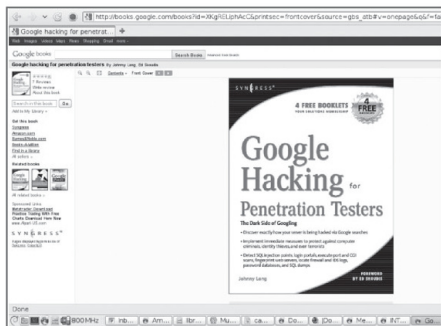


Figura 2. La popularidad de las técnicas de **Google hacking** ha llevado a la publicación de libros completos que hablan sobre el tema.

“contra el phishing, la medida más eficiente contra el phishing es la capacitación de los usuarios,

que necesitan comprender cómo pueden ser estafados y cuán fácil es crear contenidos que simulen ser de entidades de confianza, con el fin de robar sus datos.

Con respecto al robo de identidad, este suele realizarse una vez completado un ataque de phishing, aunque también existen otras formas de acceder a los datos necesarios para hacerlo. El objetivo principal aquí es suplantar la identidad de una persona para realizar compras o pagos a su nombre, generalmente, utilizando tarjetas de crédito. Este tipo de ataques es el de más alto crecimiento en los últimos años y representa un gran riesgo para todas las personas. No se

encuentra relacionado directamente con la seguridad en las organizaciones, sino más bien con la seguridad personal. Estos son algunos consejos para evitar ser víctimas del phishing:

- » Escribir a mano —no hacer clic en los enlaces— las direcciones de sitios web importantes, como entidades bancarias u otros sitios que nos soliciten información confidencial.
- » Cerrar siempre las sesiones de los sitios web y las aplicaciones confidenciales.
- » Tener en cuenta que los **bancos** y otras entidades que manejan dinero nunca nos solicitarán que les enviemos nuestras claves de acceso ni ningún otro tipo de dato confidencial.
- » Jamás utilizar máquinas de **acceso público**, como las de **cibercafés**, para enviar o recibir información confidencial.

Estos consejos, entre otros, son los que debemos comunicar a los integrantes de nuestra organización para que estén al tanto acerca de cómo evitar ser víctimas de este tipo de ataques.

SERVICIOS DE MENSAJERÍA

Podemos definir los servicios de mensajería como **servicios que permiten intercambiar mensajes entre usuarios**, lo cual es bastante



Figura 5. En el sitio web de Identidad Robada podemos encontrar mucha información acerca de los robos de identidad, cómo prevenirlos y qué hacer si pensamos que somos víctima de uno (www.identidadrobada.com).

Figura 6. El proyecto ASCII Ribbon es una campaña que busca generar conciencia acerca de las ventajas de utilizar el correo electrónico en modo texto plano, que reduce los riesgos de seguridad (www.asciiribbon.org).



genérico, por no decir súper genérico. Este tipo de servicios se ha vuelto muy popular en Internet, porque es, básicamente, la gran herramienta de comunicación entre usuarios. A medida que estos servicios fueron evolucionando, se los ha dotado de más características que potencian la cantidad de contenidos que se pueden transmitir. Recordemos que, en un principio, solamente existían mensajes en texto plano, a través del correo electrónico o el IRC. En la actualidad, contamos con varias herramientas de mensajería, de las cuales haremos un análisis de seguridad.

MENSAJERÍA INSTANTÁNEA

Los servicios de mensajería instantánea son unos de los más utilizados por los internautas, tanto en sus hogares como en las oficinas. Estos han pasado de ser un simple IRC (**chat simple**), a convertirse en herramientas y protocolos más avanzados, como ICQ, MSN Messenger, entre otros. Con esta evolución y ha surgido una gran cantidad de problemas de seguridad, que debemos tener en cuenta. Si a esto le sumamos que, actualmente, muchos sitios web cuentan con mensajería en línea, como el mensajero de Facebook, podemos obser-

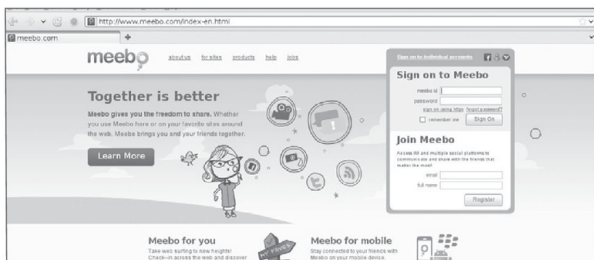


Figura 7. Meebo es uno de los sitios web que permiten, desde un único lugar, realizar conexiones con distintos servicios de mensajería. El nacimiento de estas aplicaciones web complica en gran medida el filtrado de los servicios de mensajería instantánea.

var que las posibilidades que tiene un usuario para intercambiar mensajes con otro son prácticamente ilimitadas, por lo que se vuelve una tarea muy compleja, y hasta agotadora, intentar bloquear todos estos protocolos y herramientas. Si necesitamos hacerlo, podemos simplificar el trabajo a través de algunos dispositivos **UTM**, como los desarrollados por **Fortinet**, **Watchguard** o **Checkpoint**, entre otros, que cuentan con grandes capacidades de filtrado por protocolo y aplicación.

TRANSFERENCIA DE ARCHIVOS

Uno de los grandes cambios de los servicios de mensajería ha sido la capacidad para enviar y recibir archivos. Esto ha dotado a los usuarios de una tremenda facilidad para transferir contenidos de manera instantánea, pero también es una gran posibilidad para los atacantes de mandar todo tipo de malware. Es por eso que muchas veces se critica el uso de los servicios de mensajería por los **riesgos de seguridad implicados**. El problema es que, de una forma u otra, la transferencia de archivos debe ser permitida en una organización. Y siempre es mejor que lo hagamos de manera transparente y amigable para el usuario, en vez de forzarlo a buscar métodos no

autorizados para transferir archivos, que podrían poner en peligro a nuestra empresa. Algunas de las opciones de código abierto que tenemos para bloquear la mensajería instantánea son el firewall gratuito **Untangle** (www.untangle.com), o la combinación de algunos productos, como el **proxy Squid** (www.squid-cache.org) y alguna otra herramienta de filtrado de paquetes, como **IPTables** para sistemas **Linux**.

Los mismos dispositivos de firewall nombrados en el apartado anterior tienen la capacidad de realizar análisis antimalware, bloqueo de transferencias por tipo de archivo y algunos otros filtros que pueden sernos de utilidad. En caso de que no podamos contar con estos dispositivos, podemos utilizar alguna de las soluciones de código abierto nombradas en el **Capítulo 4**.

Si bloqueamos todos los caminos a un usuario, este tratará de encontrar otros alternativos, e inseguros. Pero si le marcamos un camino correcto, va a seguirlo sin problemas

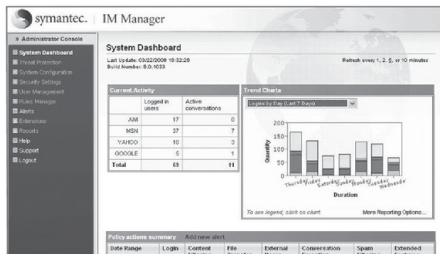
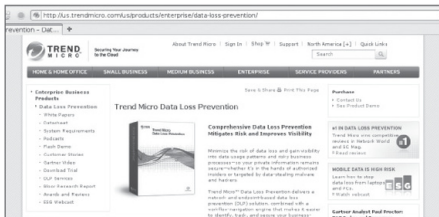


Figura 8. Algunos fabricantes, como Symantec, ofrecen productos especializados para el control de los servicios de mensajería instantánea. En la imagen, Symantec IM Manager.

Figura 9. Varios fabricantes de software de seguridad, como TrendMicro, ofrecen productos para evitar la fuga de información y la pérdida de datos (www.trendmicro.com).



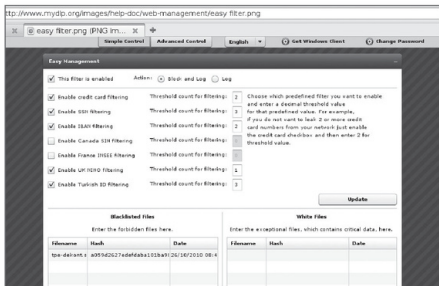
FUGA DE INFORMACIÓN

Una de las grandes preocupaciones actuales de las organizaciones con respecto a la seguridad es la **fuga de información confidencial**. Esta situación se ve agravada por la gran cantidad de medios de comunicación con los que contamos al tener una conexión a Internet. Es por eso que la fuga de información debe encararse desde varios frentes para poder combatirla adecuadamente. No estamos hablando de un dispositivo, protocolo o herramienta en particular, sino que debemos proteger una infinidad de métodos para transferir información. Es por eso que, por sobre todas las cosas, los

usuarios deben estar al tanto de qué información pueden compartir abiertamente y cuál deben mantener privada. Por lo tanto, podemos observar que

“la primera medida para luchar contra la fuga de información es la capacitación

Figura 10. El proyecto de código abierto MyDLP desarrolla un software destinado a la protección contra la fuga y la pérdida de datos. En la imagen podemos observar su uso para filtrar ciertos tipos de datos, como números de tarjetas de crédito (www.mydip.org).



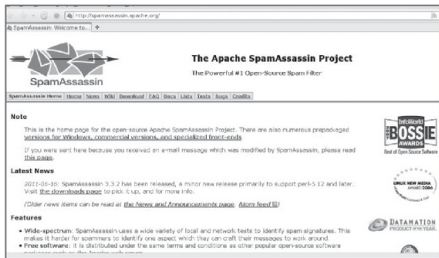


Figura 11. El proyecto de código abierto Spamassassin es el más reconocido filtro antispam. Es desarrollado por la fundación Apache y cuenta con una gran capacidad de filtrado, además de tener una amplia documentación.

COMUNICACIONES NO DESEADAS (SPAM)

Los **mensajes no deseados (spam)** han dejado de pertenecer solamente a los servicios de correo electrónico, y ahora forman parte de cualquier servicio de mensajería, aunque el correo se lleva la mayor parte de este tipo de transferencia.

Porcentaje de spam sobre el total de correos electrónicos procesados: 88,55%

(Fuente: Informe anual INTECO 2010)

En una organización, el bloqueo de spam es estrictamente necesario, porque este alcanza niveles tan altos, que reduce de manera notable

RECOMENDADOS

En el sitio web Wikipedia (http://en.wikipedia.org/wiki/Anti-spam_techniques) podemos encontrar un excelente artículo que detalla varias de las técnicas antispam más efectivas, tanto para los usuarios finales como para los administradores de servicios de correo electrónico. Esta enciclopedia libre es un recurso de gran valor para todas nuestras tareas de investigación.



Figura 12. El sitio web Spamhaus mantiene varias listas negras con dominios y direcciones IP que son frecuentemente utilizados para enviar spam. Es un excelente recurso para ayudarnos en la lucha contra el correo no deseado.

las capacidades de trabajo de los empleados porque si los obligamos a recibir enormes cantidades de spam, se pierde mucho tiempo en catalogar a mano qué es spam y qué no lo es.

VOIP

Los servicios de voz sobre IP (VoIP) se han vuelto extremadamente populares, al ofrecer mejores características y menor costo que la actual telefonía tradicional. Es por eso que su uso crece año a año y las organizaciones implementan este tipo de soluciones para reemplazar las viejas tecnologías y unificar sus redes de comunicación. Como toda tecnología, los protocolos relacionados con VoIP presentan ciertas falencias de seguridad, sobre todo, si están mal configurados. Esto podría permitir tanto la escucha de conversaciones como la realización de llamadas por

parte de terceros, que obligan a la organización a pagar por comunicaciones que no realizó.

Es por eso que, en caso de implementar VoIP en nuestra organización, debemos tomar los recaudos necesarios, y analizar tanto los protocolos que vamos a utilizar, como las herramientas y productos por implementar.

Algunos consejos de seguridad para los servicios VoIP son: encriptar las comunicaciones, revisar la seguridad de los protocolos TCP/IP que dan soporte a estos servicios y monitorear el uso de las centrales de telefonía IP.

Actualmente, la combinación de los protocolos más utilizada en los ambientes VoIP son **SIP** (*Session Initiation Protocol*) para el inicio y la terminación de llamadas, y **RTP** (*Real-time Transport Protocol*) para el transporte del audio. Es muy aconsejable emplear alguna variante encriptada de ellos, como **SRTP**, que, básicamente, es lo mismo que RTP pero con **encriptación de tráfico**.



Figura 13. En el sitio web Voip-Info (www.voip-info.org) podemos encontrar una gran cantidad de información acerca de productos, protocolos y herramientas relacionadas con la tecnología VoIP, así como también varias recomendaciones de seguridad.

ESPIONAJE DE COMUNICACIONES

Los medios físicos que transportan las comunicaciones tradicionales suelen ser, por naturaleza, muy difíciles de interceptar para capturar la información que viaja a través de ellos, debido a que esto suele producir cortes u otras anomalías en la comunicación, que son rápidamente detectables. Además, se requiere acceso físico a algún punto del medio de transporte para efectuar alguna captura. Sin embargo, en el caso de las comunicaciones IP, se vuelve muchísimo más fácil capturar información de manera remota, y es posible hacerlo sin que esto produzca un impacto negativo o extraño en la comunicación.

Existen varios programas desarrollados exclusivamente para capturar paquetes con audio, para luego ensamblarlos y obtener una copia exacta de toda la comunicación realizada. Es por eso que resulta de suma importancia la

encriptación del tráfico que contenga comunicaciones críticas o privadas. Para esto, podemos utilizar protocolos como **SRTP** (explicado más arriba), **IPSec** o algún otro tipo de enlaces del tipo **VPN**.

VIDEOCONFERENCIAS

Con la capacidad de transportar datos de audio sobre redes IP para realizar llamadas telefónicas, el salto a las videoconferencias (llamadas con video incluido) prácticamente fue sencillo, porque solo se incluye un nuevo tipo de datos, utilizando la misma arquitectura VoIP. La gran diferencia que presenta con VoIP es que este tipo de llamadas no puede ser transmitida a través de la red de telefonía tradicional (porque esta no cuenta con soporte de video).

Sin entrar en más detalles, podemos decir que todas las medidas de seguridad requeridas para VoIP se aplican a las llamadas de videoconferencia, y que debemos encriptar y asegurar los datos que transmitimos.



Figura 14. El nCite 4000, de Audiocodes, es un equipo que, entre otras cosas, provee seguridad para las comunicaciones VoIP, con capacidades de encriptación, protección contra ataques DoS, validación de protocolos y muchas otras funciones.

RECOMENDADOS

Roberto Gutiérrez Gil, Ingeniero en Telecomunicaciones de la Universidad de Valencia, ha escrito un excelente documento que repasa las tecnologías implicadas en una arquitectura de VoIP, hace un análisis de las posibles vulnerabilidades de seguridad y evalúa algunos de los ataques más comunes. Podemos consultarlo en el www.portantier.com

VIRTUALIZACIÓN

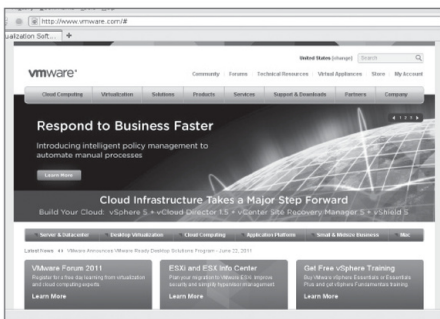
El uso de este tipo de tecnologías ha crecido enormemente en los últimos años, a tal punto que podemos afirmar que la mayoría de las organizaciones las implementa de uno u otro modo. La reducción de costos y las mejoras en los procesos de gestión que nos brinda la virtualización son evidentes, y hacen que cualquier empresa cuente con este tipo de proyectos dentro de sus planes. Nosotros debemos estar preparados para responder a las cuestiones de seguridad relacionadas con estas tecnologías.

En la actualidad, existen varios fabricantes de **plataformas de virtualización**, cada uno con sus ventajas y desventajas. La decisión de utilizar una u otra tecnología debe tomarse sobre la base de las necesidades de cada organización. También debemos considerar hacer una inversión en herramientas que nos faciliten la gestión de la infraestructura: copias de respaldo, recuperación en caliente, balanceo de cargas, etcétera. A continuación, definimos algunos de los puntos más importantes para tener en cuenta con respecto a la seguridad de infraestructuras virtuales.

ASEGURAR CORRECTAMENTE LOS EQUIPOS DE HOST

Los equipos que contienen las **máquinas virtuales** deben estar adecuadamente asegurados, debido a que una falla podría comprometer la confidencialidad, integridad o disponibilidad de todas las máquinas virtuales alojadas en ellos. También debemos recordar que los equipos host cuentan con un sistema operativo que puede ser atacado, por lo que debemos verificar con detenimiento la documentación del fabricante, a fin de configurar toda la solución como corresponde.

Figura 15. VMWare es el líder en soluciones de virtualización. Cuenta con una gran cantidad de productos, y varios de ellos, con funciones de seguridad avanzadas (www.vmware.com).



ASEGURAR LOS MEDIOS DE ALMACENAMIENTO

En las soluciones de virtualización medianas o grandes se recomienda utilizar dispositivos de almacenamiento dedicados —conocidos como **storage**— para aumentar la capacidad, la **velocidad de lectura/escritura** y las posibilidades para gestionar la información.

Si implementamos este tipo de soluciones, debemos considerar a nuestros **equipos de storage** como críticos, porque podrían exponernos a una destrucción de los datos o a la fuga de información.

“ En los ambientes virtuales, cada máquina virtual está formada por algunos pocos archivos

Si estos se ven comprometidos, un atacante podría llevarse una copia completa del sistema o destruir nuestros sistemas productivos.

ASEGURAR CADA UNA DE LAS MÁQUINAS VIRTUALES

Cada máquina virtual debe ser asegurada tal y como se lo haría en caso de que fuera una máquina física. Es importante tener esto en cuenta, porque la facilidad de crear, copiar y eliminar máquinas virtuales muchas veces genera una falsa sensación de sencillez, que lleva a algunos administradores a olvidar los procesos de seguridad.

UTILIZAR ADECUADAMENTE LAS PLANTILLAS DE MÁQUINAS VIRTUALES

Para simplificar las tareas expuestas en el punto anterior, es una buena práctica de seguridad definir una plantilla de sistema que ya cuente con todas las configuraciones necesarias, para así poder crear fácil y rápidamente otros sistemas a partir de ella.

Realmente es de suma importancia que esta plantilla esté configurada cómo corresponde, dado que un error en ella provocaría fallas en todos los servidores creados.

CONTROLAR ADECUADAMENTE LA GESTIÓN DE LA INFRAESTRUCTURA VIRTUAL

La facilidad de administración que presentan las infraestructuras virtuales muchas veces hace que cualquier persona del sector de IT cree, modifique o elimine máquinas virtuales. Esto es un gran riesgo no solo para la seguridad, sino también para el rendimiento de las máquinas virtuales. Debemos recordar que, en ambientes de producción, la creación o modificación de las configuraciones podría llevar a un consumo excesivo de recursos de hardware o a fallas inesperadas si se modifica el hardware virtual sin tener en cuenta las configuraciones necesarias para el sistema operativo que corre sobre él.

IMPLEMENTAR FILTROS FÍSICOS EN LAS ZONAS DE ALTA CRITICIDAD

Aun cuando los fabricantes de soluciones de virtualización prometen que sus productos brindan igual o mayor seguridad que las separaciones físicas, debemos considerar separar los equipos que contienen máquinas virtuales de prueba, de los que contienen máquinas virtuales críticas para la operatoria de nuestra organización. Recordemos que los ambientes de pruebas suelen ser más propensos a errores



Figura 16. El fabricante de productos de seguridad McAfee cuenta con varias soluciones desarrolladas para aumentar la seguridad en entornos virtualizados (www.mcafee.com).

o malas configuraciones, de modo que no debemos permitir que estas fallas dejen expuesta la infraestructura de producción.

En caso de que no sea posible realizar separaciones físicas, deberemos asegurarnos de aprovechar todas las características de seguridad con las que cuente la solución que estamos implementando.

LOS SISTEMAS HOST SON TAN CRÍTICOS COMO LA MÁQUINA VIRTUAL QUE CORRE SOBRE ELLOS

Es preciso recordar esto al configurar los sistemas host. Si es que vamos a alojar dentro de ellos máquinas virtuales que tengan una alta criticidad para la organización, debemos catalogar estos sistemas host con la misma criticidad que las máquinas virtuales que contienen. Como analizamos anteriormente, una falla en los sistemas host podría comprometer las máquinas virtuales que alberga.

SEPARAR UNA RED PARA ADMINISTRACIÓN, DE LA INFRAESTRUCTURA VIRTUAL

Las telecomunicaciones que corresponden a la administración, tanto de los sistemas host como de las máquinas virtuales que contienen, deben estar separadas del resto del tráfico de la red, a fin de garantizar que siempre podremos administrar de manera adecuada la infraestructura. Recordemos que una red plana, sin segmentar, podría colapsar si cualquiera de sus componentes sufriera fallas de algún tipo. Es por eso que debemos prevenir el hecho de quedarnos sin la capacidad de gestionar la infraestructura. Esto puede lograrse implementando separaciones tanto físicas, (hardware distinto), como lógicas, (distintas redes virtuales, o VLANs).

GARANTIZAR LA CONECTIVIDAD DE LA INFRAESTRUCTURA CON LAS DEMÁS REDES

Muchas veces se hace hincapié en garantizar la disponibilidad de las máquinas virtuales, implementando redundancia, tanto de software

como de hardware. Y esto está muy bien, pero también debemos considerar el caso de que el hardware de telecomunicaciones presente fallas. La pérdida de conectividad entre la infraestructura virtual y el resto de la red podría significar una pérdida total de disponibilidad de los servicios. Es por eso que precisamos garantizar el funcionamiento de la red, de ser posible, utilizando hardware redundante.

IMPLEMENTAR SEPARACIÓN DE TAREAS PARA LA GESTIÓN DE LA INFRAESTRUCTURA

Es ampliamente recomendable que por lo menos dos personas estén encargadas de gestionar la infraestructura virtual, utilizando lo que se conoce como **separación de roles**, para que ninguna desarrolle completamente las tareas de gestión. Esto disminuye de manera notable la probabilidad de errores, al requerir que al menos dos personas estén de acuerdo con los cambios que habrá que realizar.

CONTAR CON REDUNDANCIA DE EQUIPOS

Como la falla de un sistema host implica la falla de todas las máquinas virtuales que corren sobre

RECOMENDADOS

*El **National Institute of Standards and Technology** (NIST) ha publicado una excelente guía de seguridad (que podemos encontrar en <http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf>), enfocada, exclusivamente, en entornos virtualizados. El documento fue lanzado a principios del año **2011**, y también considera entornos de **cloud computing***

él, es ampliamente recomendable que implementemos redundancia de hardware o soluciones de virtualización que nos permitan contar con varios sistemas host distintos, que tengan la capacidad de suplantarse entre sí en caso de que alguno de ellos presente un problema.

CLOUD COMPUTING

Otra de las tecnologías emergentes, que nació de la mano de la virtualización, es la computación en la nube o **cloud computing**, que nos permite brindar y utilizar servicios alojados en Internet. Si bien esto permite tener una gran reducción

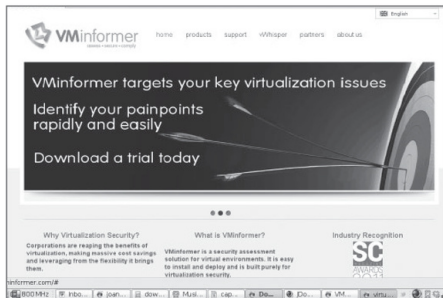


Figura 17. Existen varios fabricantes, como VMInformer, que se dedican pura y exclusivamente a desarrollar soluciones de seguridad y auditoría para ambientes virtualizados.

de costos y nuevas capacidades para brindar servicios, también es muy cuestionado desde el punto de vista de la seguridad, debido a que los equipos en los que las empresas alojan su información no pertenecen a ellas mismas, sino al proveedor del servicio. Por lo tanto, la pérdida de control sobre los datos genera un alto grado de incertidumbre, que pone en duda la viabilidad de implementar este tipo de sistemas para aquellas organizaciones que se preocupan por la seguridad. A continuación, veremos algunos de los aspectos que debemos tener en cuenta cuando utilizamos este tipo de servicios.

UTILIZAR ENCRYPTACIÓN DE DISCOS

Si la información almacenada en los discos rígidos no se encuentra encriptada, cualquier persona con acceso a ellos —sobre todo, en el caso de los discos virtuales— podría llegar a

realizar fácilmente una copia de todos los datos que contienen. Al utilizar encriptación, hacemos que solamente el sistema operativo con las herramientas y claves adecuadas pueda leer la información, con lo cual reducimos el riesgo de una posible fuga de datos.

ASEGURARNOS DE TENER COPIAS DE RESPALDO DE LOS DATOS

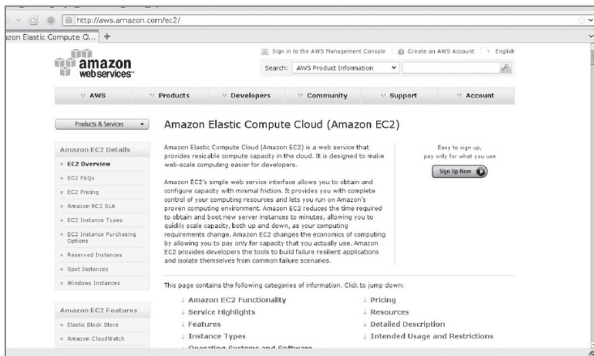
Debemos corroborar que existan copias de seguridad de nuestros datos, y que estas funcionen correctamente. Ya sea que las hagamos nosotros, o el mismo proveedor del servicio, es necesario verificar que las copias existen y pueden ser recuperadas sin problemas.

Un malentendido puede llevar a pensar que el proveedor realiza las copias de seguridad, cuando en realidad no es así, y esto puede producir pérdidas de datos críticos para las organizaciones.

Figura 19. La plataforma EC2, de Amazon, fue una de las primeras ofertas de servicios del tipo cloud computing. Cuenta con una gran cantidad de características y una probada estabilidad (<http://aws.amazon.com/ec2>).

CONTRATAR SOLO A PROVEEDORES DE CONFIANZA

Si vamos a utilizar este tipo de servicios para procesar información crítica, debemos contratar



únicamente a proveedores de confianza, y prestar mucha atención a los acuerdos de nivel de servicio y a las políticas de seguridad y privacidad que ellos utilizan, para conocer si nuestros datos estarán verdaderamente protegidos.

LA PRIVACIDAD DE LOS DATOS

En caso de que nos encontremos analizando si contratar o no servicios de computación en la nube, debemos considerar el tipo de datos que vamos a alojar y qué nivel de responsabilidad tenemos sobre ellos.

Por ejemplo, si contratamos un software que nos permite alojar toda la información de nuestros clientes, para realizar campañas de marketing, seguimiento de ventas y otras tareas, debemos tener en cuenta qué clase de datos estaremos guardando en esta plataforma, y si las políticas de seguridad y privacidad del proveedor se adecuan a nuestras necesidades. Además, dependiendo del tipo de datos con los que trabajemos, podría llegar a ser ilegal guardarlos en los equipos de otra empresa sin notificárselo a nuestro cliente. En los casos de datos personales, como creencias religiosas e historiales médicos, que están protegidos fuertemente por la ley, debe-

mos analizar cuidadosamente la viabilidad legal de este tipo de servicios. Por lo tanto, antes estas situaciones, será recomendable contratar a un abogado especializado en estas cuestiones para que pueda brindarnos una correcta asistencia y nos evite caer en problemas legales.

DIFERENCIAS CON OTROS SERVICIOS

Cabe destacar que, si bien los servicios de cloud computing pueden parecer inseguros o inapropiados para cierto tipo de tareas (y no es que no lo sean), hace años que contamos con la posibilidad de contratar otros servicios de similares características, que también podrían poner en riesgo la privacidad de nuestros datos. El ejemplo más claro y evidente son los servicios de alojamiento o hosting, en los cuales una empresa guarda sus datos en los servidores del proveedor, sin tener prácticamente ningún control de lo que se hace con ellos. El peligro que puede observarse en estos casos es que el alojamiento de datos suele ser compartido con varios clientes. Si bien ellos no deberían poder acceder a la información



Figura 19. En el sitio web de la Asociación Española para el Fomento de la Seguridad de la Información podemos encontrar, entre otros, un interesante documento llamado Guía para la Seguridad en áreas críticas de atención en Cloud Computing (www.ismforum.es).

de otro, una mala configuración de seguridad podría permitir el robo o la pérdida de datos. Aunque los servicios de alojamiento suelen utilizarse para almacenar información pública, como los sitios web, también suelen usarse para guardar todos los correos electrónicos de una organización, por lo que se estaría dando acceso a todos los mensajes al proveedor del servicio. Debemos tener en cuenta este tipo de factores no solo para la computación en la nube, sino también para cualquier servicio que requiera alojar información en equipos ajenos a nuestra organización. Por otra parte, servicios como el **housing** nos permiten llevar equipos de nuestra propiedad y conectarlos a la infraestructura de red de un proveedor, a fin de utilizar los recursos eléctricos, de espacio y de telecomunicaciones que este ofrece, pero sin que el proveedor tenga acceso directo a ellos. En estos casos, también es ampliamente recomendable utilizar encriptación de discos y contratar solo a proveedores de confianza.

TECNOLOGÍA MÓVIL

Las tecnologías móviles permiten aumentar enormemente la productividad de los empleados de una organización, al darles la posibilidad de trabajar desde cualquier lugar físico, conectándose a través de distintas redes de datos. Obvia-

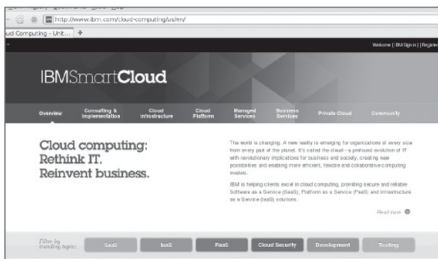
mente, esto trae aparejadas varias consideraciones de seguridad que debemos tener en mente si necesitamos ofrecer este tipo de conexiones. En los siguientes apartados analizaremos diversos factores para tener en cuenta.

DISPOSITIVOS PORTÁTILES

Los dispositivos portátiles, como smartphones, notebooks, tablets y otros, permiten a los usuarios transportar sus equipos de trabajo de manera sencilla, lo que les da la posibilidad de llevar sus herramientas laborales a cualquier sitio. Cada uno de estos dispositivos suele contar con varias opciones de conectividad (como 3G, Bluetooth, y otras), que permiten a los usuarios conectarse a distintas redes y navegar por Internet.

Esto genera la posibilidad de que un dispositivo de nuestra red se haya conectado previamente a otras redes no seguras, y que podrían haberlo infectado con malware

Figura 21. Las grandes empresas del mercado, como IBM, cada vez ofrecen más servicios relacionados con la computación en la nube (www.ibm.com/cloud-computing/us/en/).



En este aspecto, es de suma importancia cuidar la configuración de estos dispositivos, para evitar que los usuarios modifiquen ciertos parámetros que podrían poner en riesgo el sistema, evitar que puedan eliminar o deshabilitar los programas antimalware, etc. Para estos casos se vuelven muy útiles las tecnologías como NAC (analizada en el **Capítulo 5**), que nos permiten realizar comprobaciones de los dispositivos antes de permitirles interactuar con los demás componentes de una red. A continuación, podemos ver una lista de consejos básicos para asegurar este tipo de dispositivos:

- » Proteger el acceso al dispositivo mediante contraseña o huella digital.
- » Utilizar solamente aplicaciones certificadas por el fabricante del equipo.
- » Emplear algún software antimalware.
- » No guardar datos confidenciales en estos dispositivos portátiles.

En 2010 se detectó un 43% más de vulnerabilidades en dispositivos móviles con respecto a 2009

(Fuente: Symantec Internet Security Threat Report Trends)

TELETRABAJO

El trabajo remoto, o teletrabajo, forma parte de la política de muchas organizaciones. Se trata, básicamente, de permitir a los empleados el acceso a los recursos internos de la organización desde Internet, a fin de llevar a cabo sus tareas a distancia.

Esta es una opción que debemos planificar

con mucho cuidado, para evitar cualquier posible brecha de seguridad. Algunas de las recomendaciones más habituales en estos casos son las siguientes:

Utilizar tecnologías de acceso VPN: esto permite que la información intercambiada entre el dispositivo remoto y los equipos que están dentro de la organización sea transportada de manera encriptada. Así, nos aseguraremos de que permitimos solo conexiones autorizadas, ya sea a través de usuario y contraseña, certificados digitales o autenticación multifactor.

Limitar los recursos accesibles desde Internet: debido a que no es necesario que los empleados accedan a todos nuestros recursos a través de Internet, debemos asegurarnos de permitir el acceso solo a aquellos que sean estrictamente necesarios para realizar tareas laborales puntuales. Tenemos la posibilidad de hacer esto separando una red dedicada a estos servicios (similar a una DMZ).



Figura 21. Los productos de la empresa BlackBerry son algunos de los dispositivos móviles más utilizados en las empresas actualmente.

Durante el año 2010, más del 62% de las empresas sufrió la pérdida de por lo menos un dispositivo móvil

(Fuente: Symantec 2010 SMB Information Protection Survey)

Mantener las conexiones en el mínimo

posible: debemos mantener la cantidad de equipos y usuarios que pueden realizar conexiones a nuestra red desde Internet en el número más bajo posible.

ATAQUES DIRIGIDOS

En la mayoría de los casos, los **ataques** a las organizaciones suelen estar hechos por personas que buscan servicios públicos mal configurados o que están probando alguna nueva

Figura 22 *La gran oferta de computadoras portátiles y la velocidad de los enlaces a Internet han fomentado la implementación del teletrabajo como práctica común en varias empresas.*



herramienta de seguridad. Ya sea que se trate de profesionales con amplios conocimientos o de personas que solo están motivadas por un momento de curiosidad, los ataques suelen hacerse a cualquier sistema que cuente con alguna vulnerabilidad conocida.

Esto hace necesario efectuar varias pruebas sobre un sistema (generalmente, con herramientas automatizadas), de modo que si este no presenta falencias, se proceda a buscar otro distinto para atacar.

Pero existe otro tipo de ataques, en los que se define un objetivo único y se lo intenta atacar constantemente, de una manera u otra, mediante distintas técnicas y herramientas. Estos ataques en general están dirigidos a entidades financieras o a organizaciones reconocidas, con el objetivo de crear pánico o como un modo de protesta.

La gran diferencia que presentan los ataques dirigidos es que, como profesionales de la seguridad, debemos enfrentarnos con la perseverancia de los atacantes y, a veces, con una gran cantidad de ellos, lo que hace que la acción resulte mucho más peligrosa y dañina.

DENEGACIÓN DE SERVICIO (DOS)

En general, los ataques del tipo **protesta** tienen que ver más con generar una **denegación de servicio** (DoS, *Denial of Service*), que con robar o destruir información. Esto es así

MUST KNOW

Uno de los problemas más recurrentes en el uso de dispositivos portátiles es su pérdida o robo. Para protegernos contra estos peligros, debemos asegurarnos de realizar copias de seguridad de los datos que contienen, y encriptar la información que almacenan a fin de dificultar su lectura por parte de terceros.

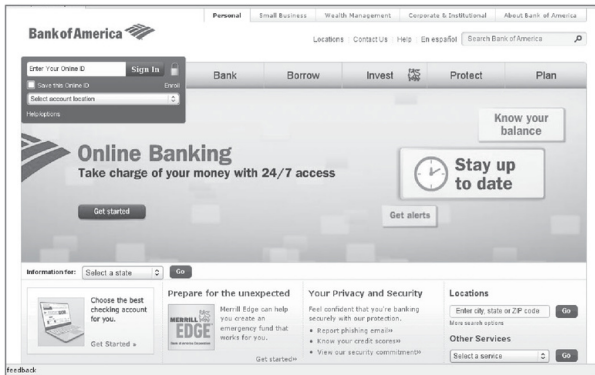


Figura 23. Las instituciones financieras de todo el mundo suelen ser el objetivo de ataques, por representar una potencial ganancia de dinero si se consigue vulnerar su plataforma de banca en línea.

porque generar un DoS suele ser relativamente sencillo si se cuenta con una cantidad suficiente de atacantes. La idea detrás de este método es agotar todos los recursos del sistema, para que este quede imposibilitado de responder a las peticiones de clientes legítimos. Si somos los encargados de asegurar una infraestructura de servicios que podría ser víctima de esta clase de peligro, deberemos tomar los recaudos necesarios e implementar los filtros correspondientes para evitar que nuestros servicios dejen de responder. En el caso de los ataques DoS o los ataques distribuidos de DoS (DDoS), la forma más eficiente de protegernos es restringir la cantidad de conexiones que un mismo cliente puede realizar hacia nuestro servidor, bloqueando cualquier conexión que exceda esos límites. Esto puede llevarse a cabo fácilmente si contamos con un firewall, ya sea un dispositivo especializado o alguna de las soluciones de código abierto basadas en sistemas UNIX. Con los tres comandos que figuran a continuación, podemos utilizar el filtrado **IPTables** de

los sistemas **Linux** para proteger las conexiones realizadas al puerto TCP/80 de nuestro equipo. Esto permitirá solo seis conexiones por minuto, lo cual restringe, principalmente, los ataques de tipo DoS. Por supuesto, habrá que ajustar estos valores de acuerdo con nuestros requerimientos.

```
iptables -A INPUT -p TCP -m state --state NEW
--dport 80 -m recent --set
iptables -A INPUT -p TCP -m state --state NEW
--dport 80 -m recent --update --seconds 60
--hitcount 7 -j DROP
iptables -A INPUT -p TCP -m state --state NEW
--dport 80 -j ACCEPT
```

Debido a que los ataques del tipo DoS son muy fáciles de realizar, debemos estar preparados para responder en forma adecuada.

EL PELIGRO DE LA PERSEVERANCIA

Cuando estamos administrando los sistemas de una entidad que puede ser de gran interés para los atacantes –generalmente, por cuestiones económicas, políticas o militares–, debemos tener en cuenta que no solo nos enfrentamos con ataques superficiales, sino que también podríamos ser el objetivo de varias semanas o meses de intentos de intrusión. Esto nos obliga a estar preparados de manera adicional, y a implementar varias tecnologías para la detección temprana de los ataques, que nos permitan bloquearlos antes de que causen cualquier tipo de daños a nuestra infraestructura.

Para estos casos, los sistemas de detección de intrusos serán un aliado fundamental en nuestra lucha contra los atacantes, porque nos permiten reaccionar de forma proactiva.

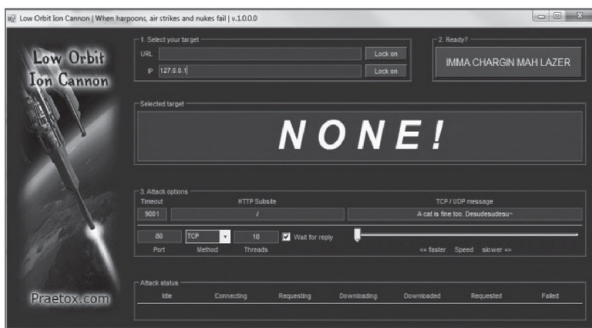
Figura 24. La herramienta LOIC (Low Orbit Ion Cannon) fue desarrollada, originalmente, para realizar pruebas de stress sobre servidores, pero muchos atacantes la han usado para efectuar denegaciones de servicio (<http://sourceforge.net/projects/loic>).

IPv6

La nueva versión del protocolo de Internet se ha hecho muy popular debido a que las direcciones del **IPv4** se están agotando, y es inminente la migración a este nuevo estándar. Entre otras cosas, **IPv6** presenta varias características de seguridad, como el uso de **IPSec** de forma nativa, resultado de analizar la vieja versión del protocolo y de la experiencia frente a los problemas de seguridad que esta contiene.

En caso de que vayamos a migrar nuestra infraestructura a IPv6, debemos considerar que esta nueva versión del protocolo no nos garantiza que no tengamos problemas de seguridad. De hecho, existen varios documentos que analizan posibles conflictos de esta índole, así que debemos estar preparados para responder del modo adecuado.

Además, si bien el protocolo IPv4 puede parecer inseguro, cuenta con la gran ventaja de haber sido probado y utilizado durante muchos años, lo cual permite conocer las falencias de seguridad y luchar mejor contra ellas. En el caso de IPv6, una implementación



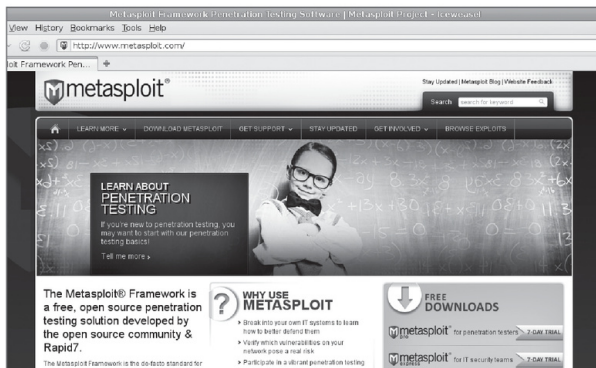


Figura 25. Metasploit es una herramienta muy utilizada para intentar penetrar en los sistemas. Cuenta con una gran cantidad de plugins para realizar diferentes tipos de ataque (www.metasploit.com).

temprana podría implicar vulnerabilidades de seguridad generadas, en particular, por el desconocimiento y las malas configuraciones, así como también por el mal soporte que algunos sistemas tienen para este protocolo.

También es preciso considerar que, si hacemos una migración paulatina, estaremos un buen tiempo conviviendo con un entorno mixto IPv4 / IPv6, lo que generará una carga adicional de gestión, y podría abrir nuevas brechas de seguridad en nuestra infraestructura.

EXPECTATIVAS PARA EL FUTURO

La seguridad informática, como profesión y como mercado, avanza constantemente. Es cada vez más evidente la importancia de la información en los negocios actuales, y eso lleva a las

organizaciones a implementar medidas de seguridad como parte de sus procesos de negocio. De la misma forma, la aparición de nuevas tecnologías impulsa la evolución de las técnicas de seguridad, que necesitan contrarrestar la gran cantidad de malware y herramientas de ataque que se generan día a día.

Todas las tecnologías mencionadas en este capítulo están relacionadas entre sí, de una u otra forma. Las comunicaciones se están unificando en las redes IP, para transmitir voz, video y datos a través del mismo medio. Esto permite abaratar costos y crear nuevas funcionalidades, que se apoyan en la movilidad de los dispositivos portátiles y el constante crecimiento en las velocidades de transferencia.

La Web se acerca cada vez más al usuario, y lo tiene como protagonista principal: ahora deja de ser un simple lector, y pasa a ser un ente de interacción, con las redes sociales y los servicios de mensajería instantánea, que buscan mantener a las personas constantemente en contacto unas con otras. Sumado a que actualmente existen muchas estafas electrónicas dirigidas a los usuarios.

Figura 26. El capítulo argentino de la Internet Society (ISOC-Ar) ha desarrollado un excelente documento llamado IPv6 para todos, que explica varias consideraciones para la implementación del protocolo IPv6 en diferentes tipos de ambientes (www.isoc.org.ar/ediciones/ipv6ParaTodos.pdf).



rios, esto hace que cada día cada individuo deba ser más responsable para no resultar víctima de ataques y robos de información, así como también para no convertirse en el puente que facilite el acceso a datos confidenciales de una entidad. Debido a la gran demanda de tráfico y a la enorme cantidad de usuarios de Internet, muchos servicios se están migrando a una arquitectura de cloud computing, y son numerosas las empresas que cuentan con sus propias nubes, formadas por servidores distribuidos a través del planeta. Esta tendencia de llevar nuestra información a servidores de otras empresas hace que

debamos tomar recaudos particulares en cuanto a qué información subimos a la nube y cuánto confiamos en las compañías que se ocupan de brindarnos estos servicios.

Toda esta enorme infraestructura en poco tiempo pasará a estar basada puramente en el nuevo protocolo IPv6, que busca solucionar varias de las limitaciones de IPv4, y permitir muchas nuevas funcionalidades. Además, promete que casi cada dispositivo electrónico cuente con una dirección IP, para poder comunicarse dentro de lo que se espera que sea un mundo totalmente interconectado. Por lo tanto, debemos familiarizarnos con los nuevos cambios que este protocolo traerá y prepararnos para utilizar las funcionalidades de seguridad correspondientes, así como también estar al tanto de las nuevas amenazas que empezarán a surgir.

Desde el punto de vista económico, las empresas no pueden darse el lujo de invertir en todos los aspectos relacionados con la seguridad, porque el presupuesto para la adquisición de software, hardware y servicios es muy limitado y debe administrarse estratégicamente. Es por eso que, como profesionales, debemos estar a la altura de las circunstancias y tener la capacidad de re-

MUST KNOW

Todos los sistemas operativos que implementaron el protocolo IPv6 tuvieron problemas en sus primeros intentos, por lo que debemos tener en cuenta este tema y verificar exhaustivamente la documentación del fabricante de la solución que vayamos a implementar. Así estaremos seguros de que el protocolo se encuentra correctamente soportado y no existen fallas conocidas.



Figura 27. El instituto INTECO ha escrito un excelente informe acerca de las implicancias de seguridad en la implementación del protocolo IPv6. Se encuentra disponible para su descarga gratuita en www.inteco.es.

comendar en qué se debe invertir para proteger adecuadamente los activos de una organización. También debemos buscar la capacitación constante, para mantenernos vigentes en nuestra profesión. Un experto en seguridad informática deja de ser un simple empleado, y pasa a ser una persona que tiene un valor muy alto en el mercado. Debemos aprovechar esta situación y hacer nuestro mejor esfuerzo por mantenernos en la élite de los profesionales, característica que es muy bien recompensada en la actualidad. Desde hace un tiempo, se han abierto muchos puestos de trabajo del tipo **CISO (Chief Information Security Officer, o Jefe de Seguridad de la Información)**. Si aspiramos a ellos, debemos contar con amplios conocimientos en las áreas de

estudio que detallamos en este libro, así como también dominar los conceptos relacionados con la seguridad física, como lo es la videovigilancia. Se trata de puestos de suma responsabilidad, muchísima emoción y un excelente salario. Esto también deja un gran margen para que las personas que recién están ingresando en el mercado de la seguridad informática puedan conseguir empleos rápidamente, ya sea

MUST KNOW

Quienes estén interesados en estudiar las causas y consecuencias del cruce de informaciones personales disponibles en la red, pueden leer el Capítulo 4 del excelente libro de Anibal Ford, La marca de la bestia. En él, este respetado comunicólogo analiza en detalle las formas de vigilancia y persuasión de las que son objetos los cibernautas.

como asistentes o juniors.

Si bien en un principio realizarán tareas básicas, son el inicio de una carrera apasionante, llena de desafíos y logros por alcanzar.

Dichos pronósticos pueden parecer futuristas, pero, hasta hace poco tiempo, los teléfonos celulares servían únicamente para realizar llamadas y enviar mensajes de texto.

“La tecnología evoluciona, y lo hace rápidamente. La seguridad informática debe hacer lo mismo, y somos nosotros los encargados de esa evolución

PARA PONER A PRUEBA

1. ¿Qué es un ataque de phishing y de qué manera puede prevenirse?
2. ¿De qué manera tenemos la posibilidad de protegernos del Google hacking?
3. ¿De qué forma podemos evitar el espionaje de comunicaciones VoIP?
4. ¿Qué debemos considerar al adquirir un servicio de cloud computing?
5. ¿De qué manera podemos defendernos de los ataques del tipo DoS?

ÁPENDICE

ETHICAL HACKING

PARA APROVECHAR ESTE CAPÍTULO

» **DESCARGAR** LA METODOLOGÍA OSSTMM (WWW.ISECOM.ORG/OSSTMM)

» **DESCARGAR** EL TOOLPACK DESDE (WWW.PORTANTIER.COM) Y PROBAR LAS HERRAMIENTAS QUE INCLUYE.

» **BUSCAR** VULNERABILIDADES EN LAS BASES DE DATOS MENCIONADAS PARA EL SOFTWARE QUE TENAMOS INSTALADO EN NUESTROS SISTEMAS.

ETHICAL HACKING

En este capítulo aprenderemos a:

Objetivo 1 Comprender los conceptos de Ethical Hacking y Penetration Testing.

Objetivo 2 Buscar vulnerabilidades desde distintas fuentes de información.

Objetivo 3 Conocer los pasos básicos para realizar un Penetration Test.

En este apéndice analizaremos las técnicas utilizadas por los atacantes para ingresar en los sistemas de forma no autorizada y veremos cómo valernos de ellas para aumentar la seguridad de nuestra infraestructura.

Los denominados **Ethical Hackers** son profesionales de la seguridad que estudian constantemente las técnicas de intrusión, así como las herramientas de ataque que suelen usarse para vulnerar los distintos sistemas informáticos. Es importante remarcar que el concepto de **Ethical Hacking**, básicamente, implica saber cómo atacar para saber cómo defender.

En ningún momento las técnicas desarrolladas a continuación deberían de ser puestas en práctica

Figura 1. OSSTMM es una de las metodologías más utilizadas para realizar Penetration Tests. Su descarga es gratuita en formato PDF en www.isecom.org/osstmm.

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

HOME EVENTS NEWS TEAM PARTNERING ABOUT US TRAINING CONTACT

TEAM ACCESS
Silver Access
Gold Access
Researcher Access

ASSOCIATIONS
Auditors (ILIA)
Training Partners
Platform Team

RESEARCH
Business Integrity (BIT)
Home Security (HSG)
Networking Protocols (NPP)
Security Auditing (OSSTMM)
Security Metrics (SM)
Child Security Awareness
Team Security Awareness
Trusted Computing (AUV)
Security Models (BOM)
Code Analysis (SCARE)
Security Tools
Reverse Engineering
CERTIFICATION
Security Analyst
Security Expert
Security Tester
Wireless Security Expert
Trust Analyst
Security Awareness Initiatives
Certified People

OSSTMM - Open Source Security Testing Methodology Manual
by Pete Herzog

OSSTMM
www.osstmm.org

The Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed methodology for performing security tests and metrics. The OSSTMM test cases are divided into five channels (sections) which collectively test: information and data controls, personal security awareness levels, fraud and social engineering control levels, computer and telecommunications networks, wireless devices, mobile devices, physical security access controls, security processes, and physical locations such as buildings, perimeters, and military bases.

The OSSTMM focuses on the technical details of exactly which items need to be tested, what to do before, during, and after a security test, and how to measure the results. New tests for international best practices, laws, regulations, and ethical concerns are regularly added and updated.

SUBSCRIBE TO ISECOM NEWS
Subscribe
VIEW ALL MAILING LISTS

NO WORRIES!
OSSTMMTRAINING.ORG

MÁS INFORMACIÓN

Existen varias certificaciones relacionadas con el Ethical Hacking. Algunas de las más destacadas son las siguientes:

- » **Offensive Security Certified Professional (OSCP)**
- » **GIAC Certified Penetration Tester (GPEN)**
- » **OSSTMM Professional Security Tester (OPST)**
- » **Certified Expert Penetration Tester (CEPT)**

para fines malintencionados y/o ilegales. Dentro de las actividades realizadas por los **Ethical Hackers**, la más conocida es la de **Penetration Testing**. Se trata, en términos simples, de simular un ataque real para analizar cuáles son las vulnerabilidades presentes en una infraestructura, a fin de poder solucionarlas antes de que una persona malintencionada se aproveche de ellas.

Contamos con varias fuentes de documentación para investigar sobre pentesting. Además, existen varias normas y metodologías que marcan algunas pautas y las mejores prácticas para llevar a cabo estos análisis. Entre las más utilizadas podemos destacar **NIST Special Publication 800-115** y **Open Source Security Testing Methodology Manual (OSSTMM)** de **ISECOM**.

CLASIFICACIONES

Según la forma en que realicemos un Penetration Test, surgirán varias clasificaciones diferentes, considerando distintos criterios. Cuando nos encontramos frente a un proyecto de este tipo, debemos tener en cuenta estas clasificaciones y dejar bien en claro cuáles serán los alcances de las tareas que se van a realizar. Además, tenemos que definir si los sistemas

se van a atacar de forma tal que podríamos llegar a provocar fallas en ellos. Estas cuestiones son muy importantes para evitar cualquier malentendido y posible disgusto con nuestros clientes o jefes. Además, es necesario que, luego de habernos puesto de acuerdo con las personas correspondientes, firmemos un compromiso legal en el que se detalle que todas las tareas por realizar son a pedido de la organización. De este modo, evitaremos varios problemas, y la organización entenderá exactamente qué es lo que se va a hacer y cómo será hecho.

EN LA PRÁCTICA PROFESIONAL

Si bien es cierto que podemos utilizar varias herramientas para automatizar el proceso de Penetration Testing, existen algunas partes del procedimiento que deben ser revisadas a mano. Debemos tener en cuenta que las herramientas automatizadas muchas veces pueden ocasionar problemas si no las configuramos de forma correcta. Así es que un buen profesional debe saber discernir entre qué tareas automatizar y cuáles realizar a mano.



INTERNO/EXTERNO

Este tipo de clasificación apunta a diferenciar los análisis según el lugar desde el cual se realizan las pruebas. Si las hacemos desde Internet, como podría realizarlas cualquier atacante desde su casa, intentaremos recopilar información sobre la empresa y de todos los servicios públicos que brinda (correo, sitios web, VPN, etc.).

En el caso de los Penetration Tests internos, nos ubicaremos dentro de la organización, directamente conectados a la red local. Eso nos permitirá tener un nivel de acceso mucho más importante, debido a que tendremos contacto con casi todos los dispositivos de la infraestructura, y no solo con los que están expuestos a Internet.

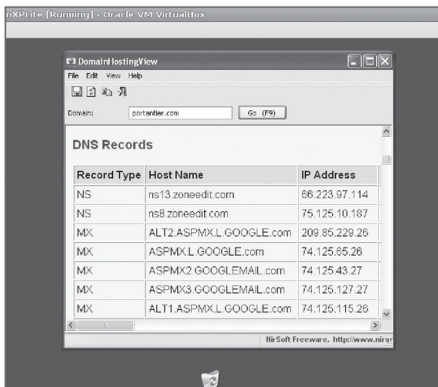
Más allá de cualquier ventaja o desventaja que presente cada modalidad, ambos tipos de análisis son necesarios. Un buen proyecto de Penetration Test debería incluir tanto un análisis interno como uno externo.

CAJA BLANCA/CAJA NEGRA

Los Penetration Tests también se diferencian sobre la base de la información compartida con el profesional que se encarga de realizarlos. Si compartimos información con el profesional, por ejemplo, acerca de las direcciones IP, la estructura de los servidores, los servicios publicados y las versiones de software que se utilizan, estamos hablando de un análisis del estilo **Caja blanca**, en el que el profesional ya cuenta con varios datos que le permitirán acelerar el proceso y realizar pruebas más específicas.

En el caso de los análisis del tipo **Caja negra**, no compartiremos ningún tipo de información con el profesional, y será este el encargado de averiguar todos los datos necesarios acerca de la infraestructura que se va a analizar. Estos análisis son los más cercanos a la realidad, debido a que un atacante tendrá que pasar por el proceso de conseguir toda la información referida a los sistemas de la compañía. La mayoría de las veces,

Figura 2. En esta imagen podemos ver que los datos arrojados por la herramienta nos permiten conocer cuáles son los servidores DNS autoritarios de ese dominio (en este caso, ZoneEdit) y cuáles son los servidores de correo responsables de ese dominio (en este otro caso, los servidores de Google).



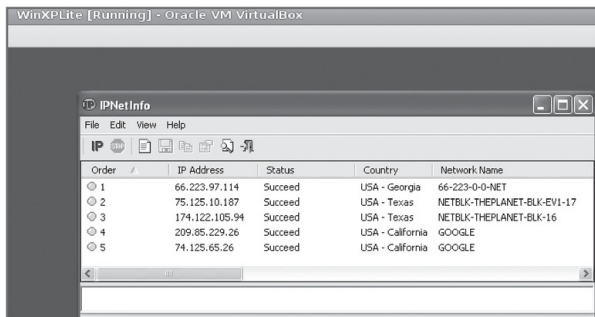


Figura 3. En la imagen vemos que todas las direcciones IP relacionadas con **portantier.com** pertenecen a equipos que se encuentran en los Estados Unidos.

las organizaciones comparten cierta información básica con el Ethical Hacker, que servirán como punto de partida para efectuar los ataques.

En estos casos en los que se comparte información, pero a un nivel muy básico, se habla de un análisis del tipo **Caja gris**.

RECONOCIMIENTO

Lo primero que debemos hacer al realizar un Penetration Test es recabar toda la información posible acerca de la organización que vamos a analizar. Para los ejemplos del resto del capítulo, evaluaremos la organización

Portantier Information Security, en la forma de Penetration Test externo y de Caja negra.

Todas las herramientas utilizadas a continuación son del tipo **freeware** o de código abierto. Varias de ellas pueden descargarse desde el sitio web **www.portantier.com** en un único paquete que no necesita instalación. Corren sobre plataformas Microsoft Windows, aunque podemos encon-

trar herramientas muy similares para cualquier sistema operativo.

Primero vamos a analizar la información provista por los servicios de DNS, utilizando **DomainHostingView**.

La misma herramienta nos brinda información acerca del servidor web en el que se encuentra el sitio principal (**www.portantier.com**). En este caso, es un servidor Linux, corriendo el software Apache HTTPD. Además, podríamos utilizar una herramienta con IPNetInfo para conocer algunos datos adicionales sobre las direcciones IP obtenidas. Con esta información, ya tenemos la posibilidad de conocer más acerca la organización que estamos analizando.

ESCAÑO

El siguiente paso en el proceso será determinar cuáles son las características de los dispositivos que utiliza la empresa en cuestión. Para hacerlo, recurriremos a un software para el escaneo de puertos, que nos permitirá conocer los detalles de puertos en escucha y software instalado en cada uno de los equipos. Una vez que hayamos utilizado dicho software, podremos obtener un

Puerto	Estado	Servicio	Versión
21/tcp	Abierto	FTP	PureFTPd
22/tcp	Abierto	SSH	OpenSSH 4.3
25/tcp	Abierto	SMTP	Exim 4.69
80/tcp	Abierto	HTTP	Apache 2.2.21
110/tcp	Abierto	POP3	Dovecot
143/tcp	Abierto	IMAP	Dovecot
443/tcp	Abierto	HTTPS	Apache 2.2.21
3306/tcp	Abierto	MySQL	MySQL 5.0.91

Figura 4. Tabla 1. Este es el ejemplo de un informe del estado de los puertos más usados en una conexión de red.

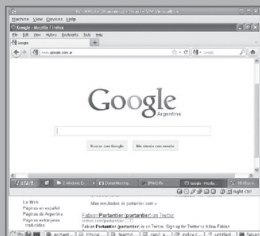
reporte muy similar al que aparece en la tabla. Aquí podemos observar que existen varios puertos abiertos y muchos servicios ejecutándose

sobre el mismo equipo, como los servicios web (HTTP y HTTPS), los servicios de correo (SMTP, IMAP y POP3), la base de datos (MySQL) y otros. Repetimos el proceso para cada una de las direcciones IP que hayamos conseguido en la etapa de reconocimiento.

EN LA PRÁCTICA PROFESIONAL

Google es uno de los recursos más importantes que podemos utilizar cuando estamos realizando un Penetration Test. Sabiendo cómo aprovechar las distintas opciones de consulta a su base de datos, es posible obtener una gran cantidad de información acerca de personas, organizaciones y dispositivos.

Existen varios libros y documentos que profundizan en el tema, conocido como Google Hacking. Esto no tiene que ver con "hackear a Google", sino con "hackear utilizando Google".



TIPOS DE ESCANEO

Existen varios métodos para verificar el estado en el que se encuentra un puerto. No todos los programas para escaneo soportan todos los métodos (Nmap si lo hace).

Escaneeo SYN: el SYN o escaneo stealth no completa el TCP three-way handshake. Un atacante envía un paquete SYN al objetivo; si se recibe de vuelta la respuesta con el SYN/ACK, se asume que podría completarse la conexión y que el puerto está escuchando. Si llega un RST desde el objetivo, se entiende que el puerto está cerrado o bien que no está activo. La ventaja de este escaneo es que suele dejar menos registros de logueo en los IDS.

Escaneeo XMAS Tree: envía un paquete con los flags FIN, URG y PSH activados. Si el puerto está abierto, este no responde; pero si está cerrado, el objetivo contesta con un paquete RST/ACK. Solo funciona sobre sistemas objetivo que cumplan con la implementación TCP/IP dada por el RFC 793 (en ninguna versión de Windows).

Escaneeo FIN: es similar a XMAS, pero únicamente



Figura 5. Nmap es el software para escaneo de puertos más reconocido. Cuenta con una gran cantidad de opciones y capacidades especiales. Es de código abierto, y está disponible para sistemas Windows, GNU/Linux y otros.

te envía un paquete con el flag FIN activado. Recibe las mismas respuestas y posee idénticas limitaciones que XMAS.

Escaneo NULL: también es semejante a XMAS y a FIN en las limitaciones y respuestas, pero envía un paquete sin ningún flag activado.

Escaneo IDLE: utiliza una IP deliberadamente modificada para mandar un paquete SYN a un objetivo. Dependiendo del tipo de respuesta, se puede determinar que el puerto está abierto o no. Esto lo hace monitoreando los números de secuencia de las cabeceras IP.

IDENTIFICACIÓN DE SERVICIOS

Algunos escaneadores de puertos permiten reconocer qué software se encuentra escuchando en un puerto y hasta en qué versión. Esto se hace a través de diversas técnicas, siendo una de las más habituales la identificación del mensaje de bienvenida obtenido al conectarse. Además, existe la posibilidad de averiguar cuál

es el sistema operativo que se está ejecutando en el dispositivo remoto, a través del envío de diversos paquetes de información y el análisis de las respuestas obtenidas (o del hecho de que no haya habido respuestas).

Nmap tiene la capacidad de realizar la detección de software y sus versiones.

ACCESO

En la etapa de acceso, intentaremos explotar posibles debilidades o malas configuraciones de los servicios ofrecidos por los dispositivos que estamos analizando.

VULNERABILIDADES

Es bien sabido que todo software tiene vulnerabilidades y otro tipo de fallas. Lo importante es quién las encuentra primero. La mayoría de las veces, las vulnerabilidades son identificadas por los propios desarrolladores del software, que liberan parches para remediarlas.

El tiempo que transcurre entre que una vulnerabilidad se hace de público conocimiento y

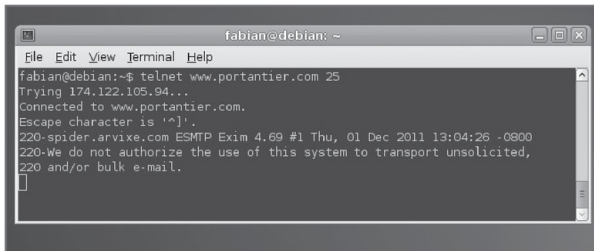


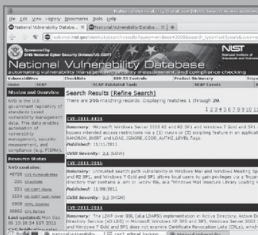
Figura 6. En la imagen podemos ver una conexión al puerto 25/tcp. Claramente, el servidor indica cuál es el software que tiene instalado y en qué versión (Exim 4.69).

EXPERIENCIA PROFESIONAL

Existen varios sitios web que podemos utilizar en nuestra tarea de obtener información acerca de las vulnerabilidades que afectan a determinados sistemas. Estos nos permiten buscar por tipo de vulnerabilidad, producto y fabricante. Algunos de los más completos e importantes son:

- <http://osvdb.org> (proyecto de código abierto)
- <http://nvd.nist.gov> (mantenido por el NIST)

En la imagen podemos observar una búsqueda dentro de la base de vulnerabilidades NVD.



que los administradores de seguridad aplican los parches correspondientes se vuelve crítico, debido a que es esa la ventana en la cual los atacantes podrían aprovechar la vulnerabilidad para acceder a un sistema.

EXPLOITS

Existen ciertas vulnerabilidades que pueden ser aprovechadas a través del uso de herramientas desarrolladas exclusivamente para ese fin, que se denominan exploits.

Dicho software suele estar desarrollado para afectar específicamente a una vulnerabilidad en particular. Su fin puede ser el de permitir ejecutar código arbitrario o, simplemente, de tirar abajo un sistema.

Los exploits pueden ser escritos empleando una diversidad de lenguajes de programación, aunque suele usarse C.

También pueden valerse de distintos tipos de ataques, tales como desbordamiento de búfer, Cross Site Scripting, Format Strings e Inyección SQL, entre otros.

INFORMES FINALES

El resultado del proceso de Penetration Test debe ser un reporte que nos permita conocer exactamente dónde estamos parados y que nos deje ver hacia dónde podemos ir con respecto a la mitigación de nuestras vulnerabilidades.

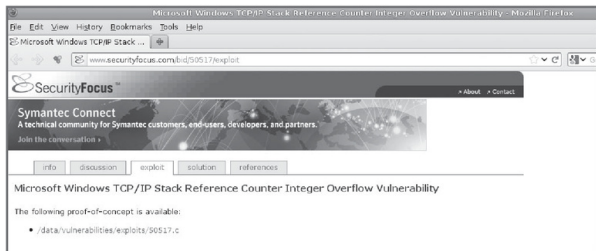
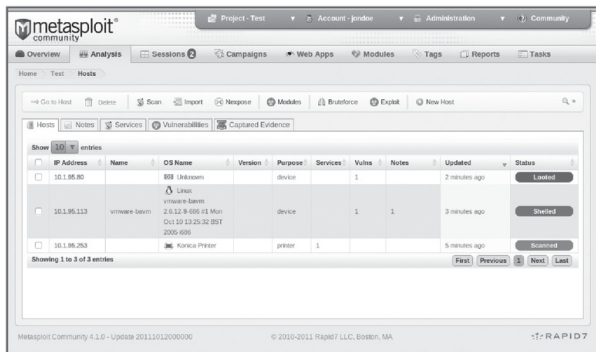


Figura 7. En la imagen observamos la búsqueda de un exploit dentro del sitio web **www.securityfocus.com**, el cual mantiene una gran base de datos de exploits y vulnerabilidades.

Es necesario comprender que un único reporte no podría ser analizado por el personal directivo de una organización y por el personal técnico. Por lo tanto, es necesario que, al finalizar el Penetration Test, obtengamos dos reportes, cada uno de ellos enfocado en un perfil diferente, un informe técnico y un informe ejecutivo.

En términos generales, ambos deben ser y estar etiquetados como confidenciales (definidas las condiciones en el acuerdo de confidencialidad firmado antes de comenzar la evaluación). Además, es preferible que sean entregados de manera impresa y en mano al responsable de la organización que contrató la tarea. Otro modo

Figura 8. Metasploit (**www.metasploit.com**) es una de las herramientas más populares para la búsqueda y utilización de exploits. Es un proyecto de código abierto, que cuenta con una versión comercial.



de mostrar los resultados suele ser mediante la realización de talleres, en los que se demuestra cuáles son las vulnerabilidades halladas y cuál podría ser el impacto de que estas fueran explotadas por un atacante.

INFORME TÉCNICO

Como es posible imaginar, el informe técnico está orientado al personal de tecnología de la organización. Por lo general, debe contener una serie de puntos comunes a todos estos tipos de análisis, aunque obviamente, esto siempre depende del consultor o empresa que lo realiza. El reporte comienza con una sección que contiene información general respecto al tipo de evaluación que se lleva a cabo y detalles como una introducción, alcance, objetivos, etcétera. Luego, el informe detalla punto por punto cada una de las vulnerabilidades encontradas, ordenadas sobre la base de la criticidad de cada una

Figura 9. Desde el sitio web www.sans.org/reading-room/whitepapers/testing podemos obtener varios documentos relacionados con Penetration Test, incluida una guía acerca de cómo confeccionar el reporte final.

de ellas. Esto permite a la organización obtener una rápida idea de cuáles son los problemas que debe resolver primero.

Por último, debe incluirse un resumen final y una lista de recomendaciones para subsanar los problemas detectados.

Es importante que también detallemos cuáles fueron las herramientas y/o metodologías empleadas para obtener los resultados, lo cual le permitirá al personal técnico efectuar sus propios análisis, ya sea para constatar cómo hicimos nuestro trabajo o para verificar si las tareas de remediación están dando resultado.

INFORME EJECUTIVO

El resumen ejecutivo está orientado a transmitir los resultados de la evaluación a la alta gerencia. Como regla general, no debe ser extenso, ya que la persona que lo leerá no suele disponer de mucho tiempo para dedicar a interpretar el material.

Se debe utilizar un lenguaje claro y poco técnico. También se deben dejar en claro cuáles serían las consecuencias directas para la organización en caso de que las vulnerabilidades encontra-

SANS InfoSec Reading Room - Penetration Testing - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SANS InfoSec Reading Room - P...

www.sans.org/reading-room/whitepapers/testing

Secure Access / Login Google Custom Search

SANS

Find Training Live Training Online Training Programs Resources Vendor About

SANS InfoSec Reading Room - Penetration Testing

← Reading Room Home

Most of the computer security white papers in the Reading Room have been written by students seeking GIAC certification to fulfil part of their certification requirements and are provided by SANS as a resource to benefit the security community at large. SANS attempts to ensure the accuracy of information, but papers are published "as is". Errors or inconsistencies may exist or may be introduced over time as material becomes dated. If you suspect a serious error, please contact webmaster@sans.org.

Featured 20 papers as of Dec 5, 2011

- OS fingerprinting with IPv6
By: Christopher Elliott (posted on September 21, 2010)
In real life human fingerprints are used as a method of identification. As of today no two fingerprints were found to be alike, hence fingerprints are an excellent way to positively identify a person beyond reasonable doubt.
- Mass SQL Injection for Malware Distribution
By: Larry Whitman (posted on April 18, 2010)
Cylons have made alarming improvements to their infrastructure over the last few years. One reason for this improvement is increased awareness to SQL injection. Malicious code writers have exploited these vulnerabilities to distribute malware.

Check Them Out!

- Cyber Defense Initiative 2011
- Security Awareness Training
- Top Cyber Security Issues
- SANS Reading Room
- Career Roadmap
- Storm Center

IBM IBM AND CONTROL OF YOUR APPLICATION SECURITY

SANS InfoSec Reading Room

cap7_ethical_hacking SANS InfoSec Reading

Mon Dec 5, 12:52 PM

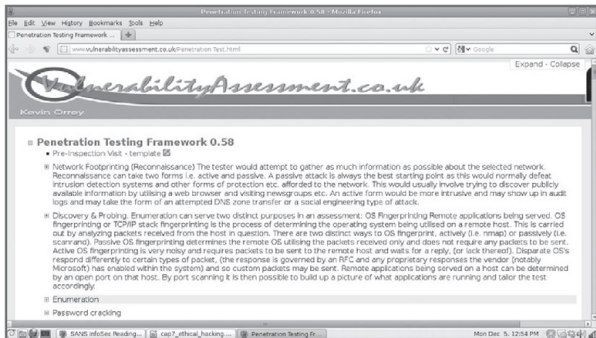


Figura 10. Desde el sitio web www.vulnerabilityassessment.co.uk podemos acceder a una guía de tareas y herramientas que podemos utilizar para la realización de un Penetration Test, así como también a una plantilla para escribir el reporte final.

das fueran aprovechadas por un atacante. Es recomendable que los datos acerca de las posibles soluciones a los problemas hallados sean expresados en costos y unidades monetarias. De esta forma, quien vaya a analizarlo tendrá como medida de relación dichas unidades. Se suele representar el impacto de la explotación de vulnerabilidades en estos términos para que quede de manifiesto el costo que le traería aparejado a la compañía no tomar medidas para reducir los riesgos asociados a esas vulnerabilidades. Para el caso de los reportes ejecutivos, se puede disponer de una exposición hablada, con proyección de estadísticas y explicaciones sobre los resultados, además de ofrecer la posibilidad de consultar y hacer preguntas en el momento. En todos los casos, además de plantearse los resultados obtenidos, es conveniente asesorar al cliente con respecto a las alternativas disponibles para resolver los problemas.

¿QUÉ SIGUE?

Las tareas relacionadas con el Ethical Hacking, como los Penetration Tests, son complejas y requieren de varias fuentes de información para llevarse a cabo de manera correcta. Es importante consultar otros documentos, así como los sitios web mencionados a lo largo de este capítulo.

Existen numerosas técnicas de ataque, que se aplican a diferentes entornos (como SQL Injection y Cross Site Scripting); y diversos conceptos que debemos tener en mente, como la evasión de medidas de seguridad (firewalls, IDS, etc.).

Por lo tanto, es necesario que nos mantengamos constantemente capacitados y leyendo acerca de las nuevas técnicas y herramientas que aparecen en el mercado.

El Ethical Hacking debe ser bien conocido por todo buen profesional de la seguridad informática. En este capítulo hemos hecho un repaso por los conceptos más importantes y hemos brindado referencias a algunos de los sitios web más destacados sobre el tema.

PARA PONER A PRUEBA

1. ¿Qué metodologías puede utilizar para realizar un Penetration Test?
2. ¿Qué es un escaneador de puertos?
3. ¿Cómo es posible identificar cuál es el servicio que se encuentra disponible en un determinado puerto?
4. ¿Qué es un exploit?
5. ¿Cuántos informes finales se deben presentar después de realizar un Penetration Test?

ÍNDICE TEMÁTICO

SERVICIOS

AL LECTOR

En este apartado, encontraremos un listado de palabras clave utilizadas en la obra. Su ordenamiento alfabético facilita el acceso directo al término buscado.

ÍNDICE TEMÁTICO

A	Agentes	124
	Aircrack	89
	Ajax	145
	Amenaza	38/42/72
	Arkela	123
	Arpalert	77
	Arpwatch	35/77/79
	AsusCERT	114
	Autenticación	83/87/97/99/117/ 125/127/128/129/132/134/136/163

B	Backup	59/95
	BCI	71
	BCP	70
	BIA	70
	Biometría	120/127
	BSD	86/105/111/113

C	CCDA	103
	CCDE	103
	CCDP	103
	CDP	81
	CEPT	173
	CERT	33/68
	Certificaciones	19
	Checkpoint	85/122/151
	CISA	21
	CISM	21
	CISO	169
	CISSP	20
	CLI	94
	Contingencia	74
	Contramedida	39
	CSS	145

D	DHCP	82/96/99
	Diameter	83
	DMZ	8/104
	DNS	100
	DomainHostingView	175
	DoS	164
	DRI	69/71
	DRP	70
	NIST	32/159/172/178
	NSA	21/82

E	EC2	160
	Estándares	48
	EventLog	131
	Exploits	178
	Exposición	38/124/181

F	Facebook	145
	FIN	177
	Firewalls	84/95/101/104/ 120/126/185
	FIRST	68
	FreeIPA	128
	FTP	100/102/128

G	Google Plus	145
	GPEN	173
	GUI	68

H	Hacking	146/147/172/173/176/181
	Hackipedia	98
	Hardening	114/117
	HIPS	137/140
	Honeyd	140

I

Honeypots	139/140/141
Host	62/90/132/156/158
HTTP	98/105

ICMP	95
IDLE	177
IDS	90/91/92
IMAP	97
INTECO	169
IPNetInfo	175
IPS	90/91
IPSec	155
IPTables	151
IPv6	166/167
IRC	150
ISC	100
ISECOM	172
ISO	16

K

Keyloggers	119
KISS	24/29

L

LAN	104
LDAP	64/87/131
LinkedIn	26/146
Linux	111/113/122/125/128/ 134/139/151/165/175/177
Logs	84/91/117/130/131/132/138
LSA	38

M

Malware	15/119
MBSA	117
MDS	130
Metasploit	179

N

MMC	135
Mobile-OTP	126
MondoRescue	125
MySQL	66/125

NAC	118/164
Nagios	61/67/134
NAI	64
NIDS	91/105/118
NIST	32/34/112/159/174/178
Norton Ghost	125
NSA	21/81
NULL	177

O

OCTAVE	33
OpenLDAP	128
OpenVAS	42/67
OPST	173
OSCP	173
OSSEC	138
OSSTMM	172

P

Parches	112/113/115/141/177
Perl	95/130
Pharming	1548
Phishing	15/100/146/148
Phishtank	148
Políticas	46/64/70/105/115/ 117/128/132/161/167
POP3	97/146/176
PSK	88
Python	27/78/95/130

R

Radius	83
--------	----

R

RANCID	94
RDP	136
Rootkits	119
Routers	78/82/89/95/101/104
RSS	145
RTP	154

S

Scripting	77
Scripts	61/78/124/130/141
SecureID	126
Servidor	105/107/110/116/ 121/124/126/128/130/136/141
SIEM	67/68/92
SIP	154
Six Sigma	30
SmartCards	125
SMTP	97/100/105/137
SNMP	36/62/77/79/93/ 96/101/107/124/137
SNMP	36/62/77/79/93/ 96/101/107/124/137
SPAM	153
Spyware	119
SRTP	154
SSH	96/136
SSID	87/135
Storage	18/59/157
Stunnel	97
Switches	77
SYN	176
Syslog	84/130

T

TACACS+	83
TCP/IP	95

T

TLS	83/97
Tokens	125
Trojanos	119
TUI	94
Twitter	145

U

UDP	83/95
UNIX	111/112/113/114/ 116/130/132/136/138/141
UTM	84/108/120/150

V

Virtualización	156
VLAN	106
VNC	136
VOIP	154
VPN	94/108/136/155/163/174
Vulnerabilidad	38/94/108/164/178
VMInformer	159

W

Webmin	137
Windows	111/112/114/115/ 116/118/119/122/128/130/132
WMI	62/133/135
WPA	87
WPE	87
WUI	94

X

XML	145
-----	-----

Z

Zabbix	61
ZoneAlarm	122
ZoneEdit	174

CLAVES PARA COMPRAR UN LIBRO DE COMPUTACIÓN

1 SOBRE EL AUTOR Y LA EDITORIAL

Revise que haya un cuadro "sobre el autor", en el que se informe sobre su experiencia en el tema. En cuanto a la editorial, es conveniente que sea especializada en computación.

2 PRESTE ATENCIÓN AL DISEÑO

Compruebe que el libro tenga guías visuales, explicaciones paso a paso, recuadros con información adicional y gran cantidad de pantallas. Su lectura será más ágil y atractiva que la de un libro de puro texto.

3 COMPARE PRECIOS

Suele haber grandes diferencias de precio entre libros del mismo tema; si no tiene el valor en tapa, pregunte y compare.

4 ¿TIENE VALORES AGREGADOS?

Desde un sitio exclusivo en la Red, un Servicio de Atención al Lector, la posibilidad de leer el sumario en la Web para evaluar con tranquilidad la compra, hasta la presencia de adecuados índices temáticos, todo suma al valor de un buen libro.

5 VERIFIQUE EL IDIOMA

No solo el del texto; también revise que las pantallas incluidas en el libro estén en el mismo idioma del programa que usted utiliza.



usershop.redusers.com

VISITE NUESTRO SITIO WEB

» Vea información más detallada sobre cada libro de este catálogo.

» Obtenga un capítulo gratuito para evaluar la posible compra de un ejemplar.

» Conozca qué opinaron otros lectores.

» Compre los libros sin moverse de su casa y con importantes descuentos.

» Publique su comentario sobre el libro que leyó.

» Manténgase informado acerca de las últimas novedades y los próximos lanzamientos.

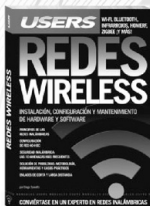
TAMBIÉN PUEDE CONSEGUIR NUESTROS LIBROS EN KIOSCOS O PUESTOS DE PERIÓDICOS, LIBRERÍAS, CADENAS COMERCIALES, SUPERMERCADOS Y CASAS DE COMPUTACIÓN.



LLEGAMOS A TODO EL MUNDO VÍA »OCA* Y **DHL****

* SOLO VÁLIDO EN LA REPÚBLICA ARGENTINA // ** VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

usershop.redusers.com usershop@redusers.com + 54 (011) 4110-8700



Redes Wireless

Este manual es fundamental para todos aquellos que quieran conocer a fondo las tecnologías inalámbricas, y así poder manejar los dispositivos y equipos de la actualidad. Para ello, veremos en detalle su instalación, configuración y mantenimiento.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1773-98-5



Trucos & secretos PC

Esta obra está dirigida a quienes dan sus primeros pasos en el uso de la PC, como también a todos los entusiastas y amantes de los móviles, los portátiles y la tecnología en general, que buscan nuevas formas de sacarles el máximo provecho a sus dispositivos.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1857-01-2



Flash: desarrollo profesional

Esta obra está destinada a todos los desarrolladores que necesitan avanzar en el uso de la plataforma Adobe Flash y sacarle su máximo provecho. A través de los distintos capítulos, se explica cómo crear un framework de trabajo personalizado.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1857-00-5



Creación de sitios web Versión 2.0

Esta obra está pensada para aprender a diseñar sitios web, sin tener conocimientos previos, a través de la última versión de la herramienta más difundida y profesional de la actualidad: Adobe CS5 Web Premium (Dreamweaver, Photoshop, Illustrator).

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1773-99-2



Java

Este libro fue concebido para ayudar a quienes buscan aprender a programar en Java, como también para aquellos que conocen el lenguaje pero quieren profundizar sus conocimientos, a través de la aplicación de buenas prácticas y las mejores técnicas.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1773-97-8



C# Avanzado

Este libro abre nuevas perspectivas para la programación de aplicaciones con C#, al llevar al lector a recorrer temas más avanzados del lenguaje y el framework .NET, con la ayuda de un catedrático experto en el tema, autor de múltiples Manuales Users.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1773-96-1



¡Léalo antes Gratis!

En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.



Administrador de redes Windows

En esta obra se presentan los fundamentos y las prácticas necesarias para la instalación y puesta en marcha de una red corporativa. El libro está centrado en WSBS 2011, un sistema operativo para servidores pensado para quienes necesitan llevar adelante soluciones de networking a bajo costo.

→ COLECCIÓN: MANUALES USERS

→ 320 páginas / ISBN 978-987-1773-80-0

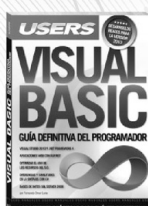


HTML 5

En esta obra se presenta un nuevo paradigma de Internet que cambia de manera sustancial el diseño y desarrollo web. A lo largo de sus capítulos, aprenderemos sobre los estándares web que existen, y conoceremos las diferencias entre las versiones anteriores y la actual del lenguaje.

→ COLECCIÓN: MANUALES USERS

→ 320 páginas / ISBN 978-987-1773-79-4



Visual Basic

Este libro está escrito para aquellos usuarios que quieran aprender a programar en VB.NET. Desde el IDE de programación hasta el desarrollo de aplicaciones del mundo real en Visual Studio 2010, todo está contemplado para conocer en profundidad el lenguaje.

→ COLECCIÓN: MANUALES USERS

→ 352 páginas / ISBN 978-987-1773-57-2



Microcontroladores

Este manual es ideal para todos aquellos que quieran iniciarse en la programación de microcontroladores. A través de esta obra, podrán aprender sobre los microcontroladores PIC 16F y 18F, hasta llegar a conectar los dispositivos de forma inalámbrica, entre muchos otros proyectos.

→ COLECCIÓN: MANUALES USERS

→ 320 páginas / ISBN 978-987-1773-56-5



Programador .NET

Este libro está dirigido a todos aquellos que quieran iniciarse en el desarrollo bajo lenguajes Microsoft. A través de los capítulos del manual, aprenderemos sobre POO, la programación con tecnologías .NET y de qué manera se desenvuelven con otras tecnologías existentes.

→ COLECCIÓN: MANUALES USERS

→ 352 páginas / ISBN 978-987-1773-26-8



Photoshop: proyectos y secretos

En esta obra aprenderemos a utilizar Photoshop, desde la original mirada de la autora. Con el foco puesto en la comunicación visual, a lo largo del libro adquiriremos conocimientos teóricos y prácticos, para conocer los efectos y herramientas que ofrece el programa.

→ COLECCIÓN: MANUALES USERS

→ 320 páginas / ISBN 978-987-1773-25-1



WordPress

Este manual está dirigido a todos aquellos que quieran presentar sus contenidos o los de sus clientes a través de WordPress. En sus páginas, el autor nos enseñará desde cómo llevar adelante la administración del blog hasta las posibilidades de interacción con las redes sociales.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-1773-18-3



Administrador de servidores

Este libro es la puerta de acceso para ingresar en el apasionante mundo de los servidores. Aprenderemos desde los primeros pasos sobre la instalación, configuración, seguridad y virtualización, hasta tener el control de los servidores en la palma de nuestras manos.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-1773-19-0



Windows 7: Trucos y secretos

Este libro está dirigido a todos aquellos que quieran sacar el máximo provecho de Windows 7, las redes sociales y los dispositivos ultraportátiles del momento. A lo largo de sus páginas, el lector podrá adentrarse en estas tecnologías mediante trucos inéditos y consejos asombrosos.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-1773-17-6



Desarrollo PHP + MySQL

Aquí se presenta la fusión de dos de las herramientas más populares para el desarrollo de aplicaciones web de la actualidad: PHP y MySQL. En sus páginas, el autor nos enseñará las funciones del lenguaje para aplicar lo aprendido en nuestros proyectos.

→ COLECCIÓN: MANUALES USERS
→ 432 páginas / ISBN 978-987-1773-16-9



Excel 2010

Este manual resulta ideal tanto para quienes se inician en el uso de Excel, como para los usuarios que quieran conocer las nuevas herramientas que ofrece la versión 2010. La autora nos enseñará desde cómo ingresar datos hasta la forma de imprimir ahorrando papel y tiempo.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-1773-15-2



Técnico Hardware

Esta obra es una completa guía para aprender a llevar adelante un correcto diagnóstico y determinar la solución más adecuada para los problemas de hardware. En sus páginas veremos todas las técnicas necesarias para implementar las soluciones de los profesionales.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1773-14-5

¡Léalo antes Gratis!

En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.



PHP Avanzado

Este libro brinda todas las herramientas necesarias para acercar al trabajo diario del desarrollador los avances más importantes incorporados en PHP 6. En sus páginas, repasaremos todas las técnicas actuales para potenciar el desarrollo de sitios web.

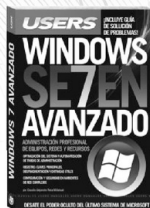
→ COLECCIÓN: MANUALES USERS
→ 400 páginas / ISBN 978-987-1773-07-7



AutoCAD

Este manual nos presenta un recorrido exhaustivo por el programa más difundido en dibujo asistido por computadora a nivel mundial en su versión 2010. En sus páginas, aprenderemos desde cómo trabajar con dibujos predeterminados hasta la realización de objetos 3D.

→ COLECCIÓN: MANUALES USERS
→ 384 páginas / ISBN 978-987-1773-06-0



Windows 7 Avanzado

Esta obra nos presenta un recorrido exhaustivo que nos permitirá acceder a un nuevo nivel de complejidad en el uso de Windows 7. Todas las herramientas son desarrolladas con el objetivo de acompañar al lector en el camino a ser un usuario experto.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-1773-08-4



Photoshop

En este libro aprenderemos sobre las más novedosas técnicas de edición de imágenes en Photoshop. El autor nos presenta de manera clara y práctica todos los conceptos necesarios, desde la captura digital hasta las más avanzadas técnicas de retoque.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1773-05-3



Grabación y producción de música

A lo largo de este libro repasaremos todos los aspectos del complejo mundo de la producción musical. Desde las cuestiones a tener en cuenta al momento de la composición, hasta la mezcla y el masterizado, así como la distribución final del producto.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1773-04-6



Linux

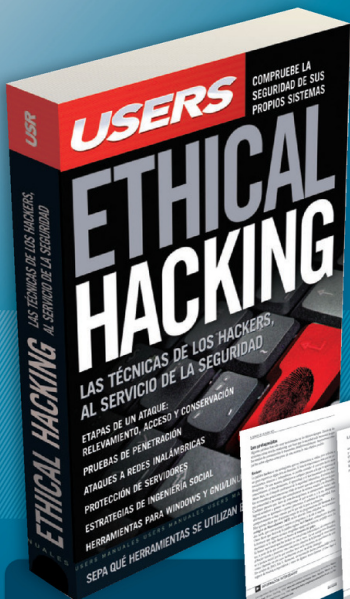
Este libro es una completa guía para mirar e iniciarse en el fascinante mundo del software libre. En su interior, el lector conocerá las características de Linux, desde su instalación hasta las opciones de entretenimiento, con todas las ventajas de seguridad que ofrece el sistema.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-26013-8-6

CONOZCA LAS TÉCNICAS DE LOS HACKERS Y CONSIGA UN SISTEMA SEGURO

Esta obra expone una visión global de las técnicas que los hackers maliciosos utilizan en la actualidad para conseguir sus objetivos. Es una guía fundamental para conseguir sistemas seguros y dominar las herramientas que permiten lograrlo.

» SEGURIDAD / INTERNET
» 320 PÁGINAS
» ISBN 978-987-1347-93-3



LLEGAMOS A TODO EL MUNDO VÍA **DOCA** * Y **DHL** **

* SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // ** VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

🌐 usershop.redusers.com // ✉ usershop@redusers.com

☎ +54 (011) 4110-8700

BIO FABIAN PORTANTIER

Fabian Portantier es un reconocido consultor especializado en seguridad informática, que dicta capacitaciones y cursos basados en las certificaciones más importantes en el área. Destacado referente en la materia en la comunidad de RedUSERS.com, ha trabajado para una gran cantidad de importantes empresas. Esto le ha dado un sólido conocimiento sobre las amenazas y vulnerabilidades que pueden encontrarse en las diferentes infraestructuras tecnológicas, así como también el conocimiento de cuáles son las mejores formas de protección para implementar en cada caso.

Fanático de GNU/Linux en general y de Debian en particular, es conocedor de varios lenguajes, como Python, Ruby, PHP y Perl; también ha trabajado con productos y tecnologías de diversas empresas, como Microsoft, Fotinet, Watchguard, Checkpoint y Cisco, entre muchas otras.

Es propietario de Portantier Information Security, consultora especializada en ayudar a las empresas con la implementación de soluciones para la protección de datos. Además, cuenta con un sitio web, www.portantier.com, en donde pueden encontrarse recursos, como artículos y software.

“ 10 minutos de capacitación
pueden reducir hasta en un 70%
los riesgos de que una persona
sea víctima de phishing ”

Fuente: www.wombatsecurity.com

SOBRE EL LIBRO

Este libro llevará al lector por un recorrido que va desde los fundamentos principales de la seguridad informática, aquellos que se emplean para escribir los documentos más reconocidos, así como también para desarrollar los sistemas de más alto nivel; hasta trucos específicos para los sistemas más utilizados en las infraestructuras tecnológicas de la actualidad.

RedUSERS

En este sitio encontrará una gran variedad de recursos y software relacionado, que le servirán como complemento al contenido del libro. Además, tendrá la posibilidad de estar en contacto con los editores, y de participar del foro de lectores, en donde podrá intercambiar opiniones y experiencias.

Si desea más información sobre el libro, puede comunicarse con nuestro Servicio de Atención al Lector: usershop@redusers.com



Information Security

Fabian Portantier is a well-known technology security consultant, teacher and owner of a consulting agency. The reader will learn how to implement solutions from Fabian Portantier expert's view.

Nivel de usuario

PRINCIPIANTE ☐
INTERMEDIO ☒
AVANZADO ☒
EXPERTO ☐

