USERS

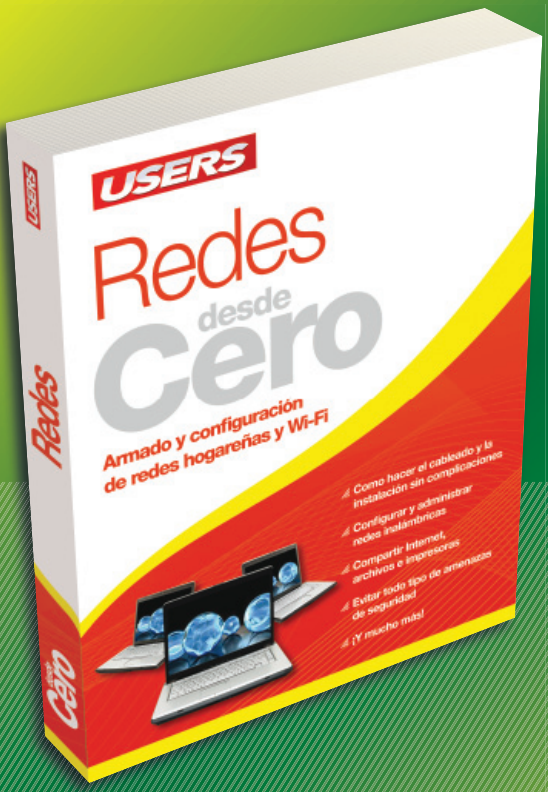
Hacking desde Cero

Conozca sus vulnerabilidades y proteja su información

- Técnicas para proteger su información
- Seguridad física y biométrica
- Amenazas en entornos web
- Ataques en redes inalámbricas
- ¡Y mucho más!

ARMADO Y CONFIGURACIÓN DE REDES HOGAREÑAS Y WI-FI

Este libro es clave para todos aquellos que quieran armar una red en su hogar. En un lenguaje sencillo y práctico aparecen todos los pasos a seguir, desde la instalación de Internet con Wi-Fi hasta la seguridad de los equipos en red.



» REDES / HOME
» 192 PÁGINAS
» ISBN 978-987-1773-02-2

SOBRE LA COLECCIÓN desde Cero

» Aprendizaje práctico, divertido, rápido y sencillo.
» Lenguaje simple y llano para una comprensión garantizada.
» Consejos de los expertos para evitar problemas comunes.
» Guías visuales y procedimientos paso a paso.

OTROS TÍTULOS DE LA MISMA COLECCIÓN

PHOTOSHOP // OFFICE // HARD
WINDOWS 7 // BLOGS // REDES
SEGURIDAD // Y MUCHO MÁS

LLEGAMOS A TODO EL MUNDO VÍA OCA * Y DHL **

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

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

Hacking desde Cero

Conozca sus vulnerabilidades y proteja su información

TÍTULO: Hacking
COLECCIÓN: desde Cero
FORMATO: 15 X 19 cm
PÁGINAS: 192

ISBN 978-987-1773-03-9

Hacking / coordinado por Daniel Benchimol. - 1a ed. -
Buenos Aires: Fox Andina;
Banfield - Lomas de Zamora: Gradi, 2011.
192 p. ; 19x15 cm. - (Desde cero; 13)
ISBN 978-987-1773-03-9

1. Informática. I. Benchimol, Daniel, coord.
CDD 005.3

RedUSERS.com

Prólogo **al contenido**

Escribir actualmente un libro sobre tecnología informática en general y sobre seguridad, en particular, es algo que parece carecer de sentido. La inmediatez con que se puede conseguir gran cantidad de información actualizada en Internet llevó a los libros técnicos casi hasta la obsolescencia. Y quien lo dice es una persona que hace más de diez años no publica un volumen en papel, en parte, convencido de esta situación y, en parte, llevado por las pocas ganas de hacer el enorme esfuerzo que significa concretar una obra de alto nivel de contenido. Pero las estructuras, reales o virtuales, existen para ser cambiadas o modificadas. Y esto es lo que han hecho mis amigos Federico Pacheco y Héctor Jara.

Cuando me dieron el honor de escribir este prólogo, desconté que se iba a tratar de una obra brillante, pues sería el producto de su capacidad y seriedad profesional. Y cuando leí los primeros capítulos, me encontré con otro factor importante: la pasión por una actividad profesional, que no es solo lo que determina la elección de una especialidad, sino que es lo que a uno lo impulsa a seguir en las noches sin dormir por estudiar o trabajar, y lo que hace que los resultados sean completos y rigurosos.

Además del grado de conocimiento y profesionalismo, es ese apasionamiento por el tema lo que llevó a Federico y a Héctor a lograr un libro, justamente, completo y riguroso para las necesidades actuales del que requiere saber de seguridad. Esto es muy difícil y hasta raro de lograr, aun en los libros escritos hace más de diez años cuando todo era mucho más fácil.

Comencé por leer con entusiasmo un extenso capítulo referido a ethical hacking, donde se presentan todos los conceptos con total precisión, y luego continué con el de Infraestructura de redes, que me resultó muy esclarecedor pese a las dificultades que plantea el tema. Este impulso me provocó leer el resto del libro en una mañana.

Retomo un concepto de dos párrafos anteriores: éste es un libro para el que necesita saber de seguridad, independientemente de cuál sea su posición profesional o académica al respecto.

En este volumen están desarrollados los conceptos básicos con los que se trabaja en seguridad informática a fines de la primera década del siglo XXI, algo muy difícil, de lograr.

El libro **de un vistazo**

Este libro plantea de forma clara y amena los fundamentos de la seguridad informática orientados al ethical hacking. No pretende ser un conjunto de tutoriales con pasos predefinidos, como si se tratara de una receta de cocina para utilizar determinada aplicación, sino que se propone profundizar en conceptos y detalles.

CAPÍTULO 1
INTRODUCCIÓN

Nos introduciremos en el mundo de la seguridad informática y algunas temáticas relacionadas. Explicaremos los términos más utilizados, las mejores prácticas y la necesidad de mantenernos actualizados. Entre otras cosas, veremos la nomenclatura y los términos más utilizados.

CAPÍTULO 2
ESPIONAJE CORPORATIVO

En este capítulo, estudiaremos la realidad del espionaje corporativo. Además, analizaremos los aspectos más importantes de la informática forense, una ciencia en pleno desarrollo.

CAPÍTULO 3
ETHICAL HACKING

En este capítulo, sentaremos las bases del ethical hacking, su terminología y los conceptos asociados, para luego centrarnos en las características de un ethical hacker, los tipos de ataque y los testeos de seguridad. Finalmente, presentaremos algunas organizaciones internacionales relacionadas con tecnología y seguridad.

CAPÍTULO 4
SEGURIDAD FÍSICA Y BIOMETRÍA

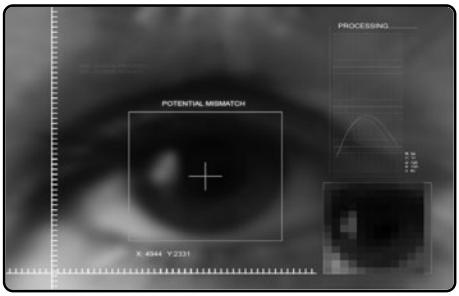
En este capítulo, veremos los conceptos relacionados con los procedimientos de control para protección de las amenazas físicas, como la biometría y las medidas de protección de accesos, así como también el monitoreo físico dentro y fuera del centro de cómputos.

CAPÍTULO 5
AMENAZAS EN ENTORNOS WEB

En este capítulo, nos dedicaremos enteramente al mundo web y a sus problemas asociados. El especial foco que hacemos sobre esto tiene su razón en el hecho de que la Web funciona como base para muchas cosas, y es por esto también que los hackers le prestan tanta atención. En definitiva, el mundo del puerto 80 requiere un especial cuidado.

CAPÍTULO 6
INFRAESTRUCTURA DE REDES

En este capítulo, abordaremos la temática de las redes de comunicaciones. Introduciremos algunos conceptos de técnicas de ataque que combinadas dan lugar a ataques más complejos. Por otro lado, haremos referencia a las distintas tecnologías y dispositivos de seguridad.



CAPÍTULO 7
MARCO LEGAL

En este capítulo, haremos una breve reseña del panorama jurídico, en una primera instancia a nivel internacional y luego puntualizaremos en el caso de la legislación argentina. Además, mencionaremos y comentaremos brevemente cuáles son las leyes relacionadas con la seguridad de la información.

CAPÍTULO 8
PENETRATION TESTING

En este capítulo, comenzaremos definiendo algunos conceptos clave de la seguridad informática y analizaremos, brevemente, distintos tipos de análisis de seguridad. Luego, nos centraremos en el Penetration Testing y veremos sus distintas fases: reconocimiento, escaneo, enumeración, acceso y, finalmente, mantenimiento del acceso.

CAPÍTULO 9
METODOLOGÍAS DE ANÁLISIS

En este apartado, veremos las tres principales referencias metodológicas utilizadas para el análisis de la seguridad informática. Las metodologías funcionan como guías para realizar determinados objetivos, e implican una serie de métodos que son procedimientos para alcanzar el objetivo, y la metodología es el estudio del método en sí.

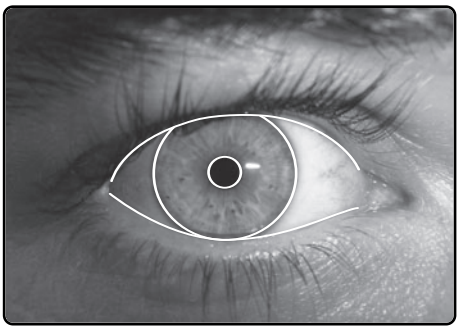
SERVICIOS
AL LECTOR

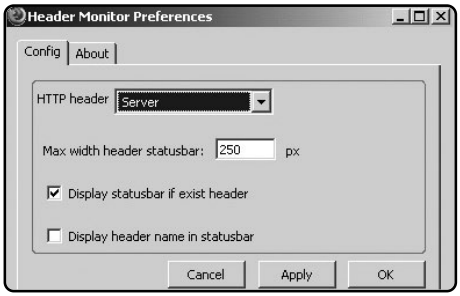
En esta última sección, encontraremos un listado de programas y sitios web recomendados, además de un índice temático de los temas tratados.

Contenido **del libro**

CAPÍTULO 3 ETHICAL HACKING 047

CAPÍTULO 4 SEGURIDAD FÍSICA Y BIOMETRÍA 063





Introducción **a Hacking**

Lejos de definiciones formales, la seguridad informática propone un modo distinto de ver la realidad, una perspectiva diferente, casi una filosofía de vida. Es una disciplina en la que resulta imposible adentrarse sin recurrir al sentido de la curiosidad y la creatividad. Desde ese misterioso lugar es que, capítulo tras capítulo, hemos intentado transmitir una parte de nuestra experiencia, la llave de una puerta que una vez atravesada nunca podrá ignorarse, el mapa de un camino que solo habrá de recorrerse con pasión y determinación.

De ningún modo hemos pretendido escribir un texto bíblico ni un conjunto de información novedosa, sino más bien un manual de consulta y de referencia, serio y de calidad, con recursos bibliográficos navegables por la web y con contenidos amenos y atractivos que fomenten su fácil lectura, tanto para quienes recién se inician en el tema como para aquéllos que ya conocen algo de él.

A lo largo de los capítulos, hemos intentado cubrir los temas fundamentales que hacen a la seguridad informática orientada al ethical hacking: comenzamos por la más elemental introducción a los conceptos necesarios, pasamos por la explicación de las distintas fases de un ataque (subdividida en etapas más simples) y por el mundo de Internet y las tecnologías web, hasta que llegamos a temas más específicos, como el control de accesos, o más amplios y complejos, como las infraestructuras de red.

También abordamos aspectos menos técnicos, pero no menos importantes, en un capítulo especialmente dedicado a los ataques sin tecnología.

Somos conscientes de que existe una gran cantidad de temas que han tenido que quedar fuera de esta obra y esa selección ha sido uno de los desafíos más complicados que tuvimos que enfrentar, por lo que incluso nosotros somos los primeros que nos hemos quedado con ganas de más.

Sin más preámbulos, les damos la bienvenida al vasto universo de la seguridad informática y esperamos que este libro sea de su agrado.

Capítulo 1
Introducción

Nos introduciremos en el mundo
de la seguridad informática
y conoceremos los términos más utilizados.

Introducción

En este capítulo, nos introduciremos en el mundo de la seguridad informática desde distintos ángulos y atravesaremos diferentes temáticas, algunas de índole más tecnológico y otras con menor contenido técnico. Entre otras cosas, veremos la nomenclatura y los términos más utilizados, y presentaremos algunos conceptos relacionados, que nos permitirán encarar el resto de los capítulos de forma amena.

Conceptos de seguridad **informática**

Tal vez una de las formas más elegantes de expresar la idea de seguridad informática sea la siguiente: un conjunto de medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, la integridad y la disponibilidad de los recursos informáticos. Destacamos la elegancia de la definición, dada la gran cantidad de conceptos que incluye y la amplitud del espectro de conocimientos que pretende abarcar.

SEGURIDAD DE LA INFORMACIÓN

En los últimos años, la vigencia de los temas referidos a seguridad informática comenzó a extenderse a otras áreas, tal es así que trascendió las fronteras de la informática propiamente dicha, elevó de alguna manera su horizonte de responsabilidad y consituyó el nuevo concepto de **seguridad de la información**. Esto se basa en que la información va mucho más allá de la netamente procesada por equipos informáticos y sistemas, es decir, también abarca aquello que pensamos, que está escrito en un papel,

BIBLIOGRAFÍA Y REFERENCIAS

Gran parte de la información de esta sección fue obtenida en los sitios web de **IBM Internet Security Systems** (www.iss.net) y **Laboratorio ESET** (http://blogs.eset-la.com/laboratorio), que tienen contenido orientado a evitar que no se cumplan las buenas prácticas.

que decimos, etcétera. De esta manera, podemos determinar que este concepto incluye al anterior como caso particular, por el hecho de agregar otras áreas de dominio. Algunos temas no relacionados directamente con la informática, pero sí con la información, son, por ejemplo, los que tienen que ver con planes de contingencia y continuidad de negocios, valuación de activos, leyes y normas, políticas y procedimientos, etcétera.

En este libro, elegiremos un enfoque específico sobre los temas técnicos que sí están estrictamente vinculados con la informática, por lo que no incluiremos más que comentarios o anexos sobre otros tópicos.

DEFENSA EN PROFUNDIDAD

En el área militar (lamentablemente la base histórica de la tecnología para su crecimiento y desarrollo), se utiliza el término **defensa en profundidad** para denotar el uso de varias líneas de defensa consecutivas, en lugar de una única barrera muy fuerte. Las ideas de su implementación teórica se basan en que un potencial enemigo perderá fuerzas al superar cada barrera, dispersará sus recursos y potencia, y se debilitará. Así, quien se defiende puede centrar sus esfuerzos en la reorganización y en la acción estratégica. En nuestro área, tomamos prestado este concepto para aplicarlo a los sistemas informáticos.

A fin de ampliar estos términos, recomendamos fuertemente la lectura de un documento, que ha sido traducido al español, creado por la **Dirección Central de la Seguridad de los Sistemas de Información del Gobierno Francés** (SGDN/DCSSI), cuyo sitio web es **www.ssi.gov.fr**.

Un extracto de dicho documento enuncia: "La defensa en profundidad del sistema de información es una defensa global y dinámica, que coordina varias líneas de defensa que cubren toda la profundidad del sistema. El término profundidad debe entenderse en su sentido más amplio, es decir, en la organización del SI, en su implementación y, por último,

en las tecnologías utilizadas. Se trata, por lo tanto, de permitir acciones de neutralización de los atentados contra la seguridad, al menor costo, mediante la gestión de los riesgos, un sistema de informes, la planificación de las reacciones y el enriquecimiento permanente gracias a la experiencia adquirida".

Para aplicarlo a los sistemas, nos podemos basar en el modelo definido por **Microsoft** y difundido a través de sus múltiples canales de entrenamiento. Elegimos este modelo por ser muy didáctico y clarificador. Éste se extiende a lo largo de varios niveles. Modelo de defensa en profundidad propuesto por Microsoft:

- Políticas, procedimientos y concientización.
- Seguridad física.
- Seguridad del perímetro.
- Seguridad de la red.
- Seguridad del equipo.
- Seguridad de las aplicaciones.
- Seguridad de los datos.

En conclusión, el uso de las técnicas de defensa en profundidad puede ayudar a implementar la seguridad de manera efectiva.

LOS PROTAGONISTAS

Algunas palabras han sido muy mencionadas en los últimos tiempos. Detrás de los términos existe

mucho marketing, que hace que la sociedad toda reconozca lo que los medios de comunicación le transmiten, desafortunadamente. Intentaremos arrojar luz sobre algunos conceptos, de una manera lo más objetiva posible.

Hackers

La palabra **hacker** es un neologismo, que en informática se utiliza para referirse a un gran experto en algún área de dominio. Si bien lo relacionamos más con los conocimientos técnicos e informáticos, es posible extender el concepto hacia otras disciplinas. De esta manera, definimos a cualquier persona a la que le apasiona el conocimiento, el descubrimiento, el aprendizaje y el funcionamiento de las cosas.

La palabra hacker es un neologismo, que en informática se utiliza para referirse a un gran experto en algún área de dominio

Ahora bien, en el mundo profesional de la seguridad informática, el término hacker se considera prácticamente un título de honor, que solo es otorgado por la propia comunidad a personajes que contribuyeron de manera notable a su desarrollo.

Cualquier persona que, fuera de estas dos acepciones, se autodenomine hacker, únicamente logrará asombrar a quienes no comprendan de qué se trata y, a la vez, demostrará abiertamente su ignorancia a quienes pertenecen al ambiente de la seguridad.

Este comportamiento no es poco común, por lo que vale la pena la aclaración. Hay quienes dicen que el término surgió de los programadores del **Instituto Tecnológico de Massachussets** (**MIT**) en los años 60. Éstos utilizaban los denominados *hacks*, que eran mejoras y trucos en programas, y de allí el nombre. Otros dicen que deriva de la palabra inglesa *hack* (**hachar**), empleada para describir la forma en que algunos técnicos arreglaban equipos electrónicos: un golpe seco. En electrónica se le suele llamar en broma **el teorema del golpe**.

INFORMACIÓN INTERESANTE

Los siguientes libros resultan útiles para conocer el marco histórico de los hackers: *Hacker Crackdown* (Bruce Sterling, 1992) **www.mit.edu/hacker/hacker.html** y *Hackers, Heroes of The Computer Revolution* (Steven Levy, 1996) **www.gutenberg.org/dirs/etext96/hckrs10.txt**.

Es bueno mencionar que los hackers no son piratas informáticos, ni cometen delitos, a pesar de lo que contrariamente se cree a veces. En un sentido más filosófico, el hacker tiende a promover una conciencia colectiva de la libertad de conocimiento y justicia social, por lo que muchas veces se los encuentra en situaciones de activismo (llamado en este caso *hacktivismo*) en pos de dicha ideología.

En octubre de 2003, Eric S. Raymond, un reconocido hacker perteneciente a la categoría de históricos especialistas y autor de algunos textos famosos (*¿Cómo llegar a ser hacker?* y *La catedral y el bazar*), propuso el emblema hacker, alegando la unificación y un símbolo reconocible para la percepción de la cultura hacker, y definió el **planeador** (*glider*), una formación del *Juego de la vida* de John Conway (**Figura 1**).

Tal vez el hacker más conocido de la historia sea **Kevin Mitnick**, arrestado en 1995 tras ser acusado

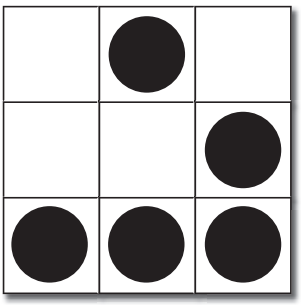


FIGURA 1. Según el creador del emblema hacker, su uso expresa la solidaridad con los objetivos y valores de un hacker.

de entrar en algunos de los servidores más seguros de Estados Unidos, aunque ya había sido procesado judicialmente en 1981, 1983 y 1987 por diversos delitos electrónicos.

El caso de Mitnick alcanzó una gran popularidad entre los medios por las estrictas condiciones de encarcelamiento a las que estaba sometido, aislado del resto de los presos y bajo la prohibición de realizar llamadas telefónicas por su supuesta peligrosidad. Finalmente fue puesto en libertad en el año 2002 (**Figura 2**).

FIGURA 2. La historia de Kevin Mitnick fue llevada al cine en la película Takedown**, aunque relata los hechos de manera tendenciosa.**

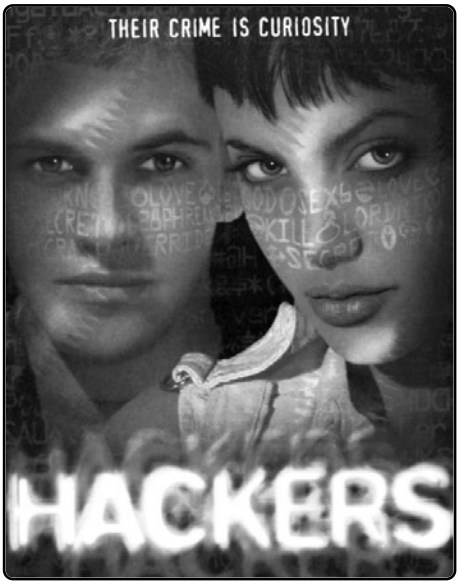
La lista de nombres históricos merecería un apartado especial, dado que se hace imposible evitar la mención de los muchos precursores que hubo pero, para los más curiosos, es posible encontrar mucha información en Internet.

Crackers

El término **cracker** proviene del vocablo inglés *crack* (**romper**). Aplicado a la informática, podemos decir que es alguien que viola la seguridad de un sistema de forma similar a un hacker, solo que ilegalmente y con diferentes fines. También se aplica específicamente al software: denotando a aquellas personas que utilizan la ingeniería inversa sobre éste, con el objetivo de desprotegerlo, modificar su comportamiento o ampliar sus funcionalidades originales.

Otros personajes

Entre los protagonistas de esta película, además de los ya vistos hackers y crackers, también se encuentran otros actores, cuyos nombres se leen de entre las páginas del ciberespacio. Podemos encontrar algunos términos como: **newbie**, que significa principiante; **lammer**, persona que presume tener conocimientos que realmente no posee; **phreaker**, hacker orientado a los sistemas telefónicos; y **script kiddie**, quien utiliza programas creados por terceros sin conocer su funcionamiento.



El conocimiento **es poder**

La frase popularizada por Sir Francis Bacon: *Knowledge is power*, que significa **El conocimiento es poder** y que deriva, a su vez, del latín *Scientia potentia est,* se refiere al hecho de que a partir del

RECURSOS EN ESPAÑOL I

Segu-Info (**www.segu-info.com.ar**) es un blog argentino con noticias, eventos, descargas y foros. **HispaSec** (**www.hispasec.com**) es responsable de la lista de correo **una-al-día**, a través de la cual los suscriptores reciben diariamente un e-mail con noticias sobre seguridad.

conocimiento podemos mejorar nuestras habilidades o adquirir otras nuevas. Si contextualizamos esta máxima y todo lo que conlleva al ámbito de la tecnología, coincidiremos en que es indispensable contar con el saber adecuado en el momento oportuno. La velocidad con la que avanza el mundo no da tregua para atrasarse, por lo cual se hace indispensable disponer de los medios para estar actualizado y con fuentes de información de confianza.

MANTENERSE INFORMADO

Como mencionamos anteriormente, estar informado es una necesidad imperiosa. No podemos darnos el lujo de desconocer las últimas noticias o novedades relacionadas con el mundo de la tecnología en general y de la seguridad de la información en particular.

Sería un poco inverosímil si nuestros conocidos supieran que nos manejamos en el ambiente de la seguridad y nos preguntasen sobre alguna noticia o tema de actualidad y nosotros no supiéramos de qué nos están hablando. Y esto es extensible a todos los ámbitos en los que nos manejemos. Por otro lado, al momento de informarnos, es bueno sentirnos identificados con la fuente de la cual tomamos la información. La fuente puede ser muy buena, pero si no nos llega el contenido, si no tenemos afinidad con la forma en que está expresado y planteado, es bastante probable que no tengamos continuidad e incluso que nos sintamos un poco desilusionados.

Para hacerlo más gráfico, podemos hacer algunas analogías con cosas cotidianas. Imaginemos que vamos a consultar a un médico que se graduó con honores de la mejor facultad de medicina, que realizó innumerables seminarios y cursos de especialización y que es reconocido en su ambiente. Sin embargo, al momento de ir a la consulta, no es lo que esperábamos. No vamos a dudar de su idoneidad, pero si no nos sentimos cómodos, no obtendremos los mejores resultados. Algo similar sucede cuando queremos aprender algún instrumento musical. Puede ser el mejor pianista, guitarrista, etcétera, pero si no tenemos afinidad con su estilo, su forma de transmitir el conocimiento o su metodología, no vamos a obtener

RECURSOS EN ESPAÑOL II

CriptoRed (**www.criptored.upm.es**) es la Red Temática Iberoamericana de Criptografía y Seguridad de la Información de la Universidad Politécnica de Madrid. Contiene presentaciones, *whitepapers* y aplicaciones. Su eminente cerebro es el Dr. Jorge Ramió Aguirre.

La necesidad de actualización está íntimamente relacionada con el hecho de mantenernos informados

los resultados esperados. Por eso es recomendable que, en un principio, leamos todo lo que podamos de todas las fuentes de información confiable que encontremos. Solo así será posible elegir con cuál de ellas nos sentimos más cómodos y cuál nos resulta más amena.

Otro punto a tener en cuenta es que mucha información actualizada está en inglés. Si bien es fácil de comprender y no presenta dificultades asociadas al idioma, debemos mejorar nuestro nivel de inglés de cara a comprender cada vez más y mejor las fuentes de información en este idioma.

NECESIDAD DE ACTUALIZACIÓN

La necesidad de actualización está íntimamente relacionada con el hecho de mantenernos informados. Como bien dijimos, la tecnología y la seguridad informática avanzan tan rápido, que es indispensable no solo estar informado, sino también actualizado. Y aquí debemos establecer una solución de compromiso. Evidentemente, no es posible estar 100% actualizado en todo, por lo que surge la necesidad de elegir, de poner prioridades sobre lo que vamos a mantenernos actualizados.

Respecto a las fuentes necesarias, en principio son las mismas que las que nos permiten estar informado, pero hay que agregar también otras más específicas. Desde el punto de vista técnico, es fundamental leer regularmente bibliografía relacionada y publicaciones (de nuevo, la mayoría en inglés). Es importante tomarnos el proceso de aprendizaje constante con humildad y saber que hay mucho por aprender, y que lo que podemos conocer es únicamente la punta del iceberg de una disciplina mucho más compleja y apasionante.

Por otro lado, una buena práctica para estar actualizado es conectarnos con asociaciones vinculadas con la seguridad de la información, grupos o foros de Internet (siempre teniendo especial cuidado del origen de dichos grupos), y todo punto de contacto con personas relacionadas con esta disciplina.

El intercambio con colegas es fundamental, ahí es donde podemos obtener la experiencia de campo,

RECURSOS EN ESPAÑOL III

Kriptópolis (**www.kriptopolis.org**) es un histórico sitio y blog en español dedicado a la criptografía y a la seguridad. Dispone de un foro donde se tratan diversas temáticas como ser: migración a sistemas operativos libres, seguridad, cortafuegos y otros temas de debate.

conocer nuevas metodologías, formas alternativas de resolver los mismos problemas, etcétera.

FUENTES CONFIABLES

De la misma manera que es indispensable estar informado y actualizado, también es fundamental contar con fuentes que sean confiables. Gracias a Internet, el conocimiento está al alcance de mucha más gente. Es relativamente sencillo encontrar datos sobre prácticamente cualquier tema, solamente a partir de Internet y de **Google** (o nuestro buscador favorito). De ahí la frase: "si no lo sabe Google, no lo sabe nadie". Como contrapartida, con tanta disponibilidad, no solamente hay información útil, sino que muchas veces lo que encontramos no es fiable. Una buena aproximación de esto sería la **Biblioteca de Babel**, descripta en un cuento de Jorge Luis Borges donde, debido a como está construida y la información que alberga, es más complicado encontrar información útil que información espuria (**Figura 3**).

Respecto de la confiabilidad de las fuentes de información, tenemos algunas maneras de ver cuáles son seguras y cuáles no (**Figura 4).** Entre otras cosas: el período de actualización, los comentarios de los demás profesionales, las opiniones de otros sitios, el ranking de los buscadores, y el posicionamiento en los sitios de *bookmarks*.

FIGURA 3.
El sitio web de Segu-info es uno de los más completos portales en español sobre seguridad informática.

RECURSOS EN INGLÉS I

SlashDot (**http://slashdot.org**) es un sitio con noticias de actualidad sobre tecnología, en categorías como *Askslashdot*, *Books*, *Interviews*, IT y Linux, entre otras. **Security Focus** (**www.securityfocus.com**) es uno de los sitios de mayor prestigio del ambiente.

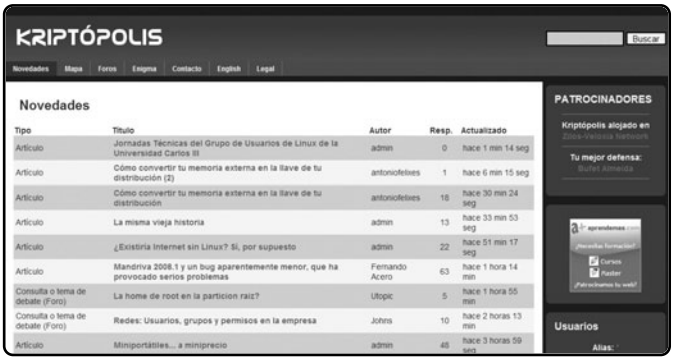


FIGURA 4.
Kriptópolis es un sitio español que funciona desde 1996 y aporta valiosa información a la comunidad.

En estas páginas, hemos descripto algunas fuentes confiables de las que nos podemos nutrir asiduamente, tanto en inglés como en español (**Figura 5**). Como comentamos al principio de esta sección, sería bueno conocerlas todas, e intentar sentir con cuál hay más afinidad y comodidad.

FIGURA 5.
Securityfocus es uno de los sitios más respetados, y cuenta con decenas de listas de distribución.

RECURSOS EN INGLÉS II

SecuriTeam (**www.securiteam.com**) es un sitio dedicado a la divulgación de noticias, alertas de seguridad, exploits y herramientas, tanto del mundo Linux como del mundo Windows. También es posible suscribirse para recibir información por e-mail.

Las buenas prácticas que no siempre **se cumplen**

Es sabido que seguir metodologías y buenas prácticas respecto de la seguridad da buenos resultados. Sin embargo, también es una realidad que éstas no siempre se cumplen en las organizaciones. A continuación, daremos un vistazo a vuelo de pájaro por algunas de las buenas prácticas, que ofrecen como valor agregado la posibilidad de reducir naturalmente la "superficie de ataque" en los sistemas.

LA ADMINISTRACIÓN SEGURA

Quizás ésta sea una de las buenas prácticas más difíciles de implementar por los administradores. Algunos de los ítems que tiene en cuenta la administración segura los comentaremos en el transcurso de los siguientes párrafos. Uno de los puntos principales es utilizar solamente el usuario **`administrador`** cuando sea estrictamente necesario. Muchos administradores, por comodidad, tienen la costumbre de usar para todo el usuario **`administrador`**. Esto trae asociados muchos riesgos, ya que si algún proceso se ve comprometido, si está ejecutado por este usuario, quien haya comprometido dicho proceso poseerá los privilegios de aquél. Otro punto importante de la administración segura es la correcta **gestión de actualizaciones**, **parches**, **hotfixes**, que trataremos posteriormente. Las buenas prácticas recomiendan un estadio donde se pruebe el impacto de estas actualizaciones, parches y demás. Desde una perspectiva más técnica, también debemos tener en cuenta el **hardening** de los servidores de la organización. El proceso de *hardening* consiste en ajustar las características propias de un sistema de forma tal que se aumente su nivel de seguridad. Algunos de los ajustes que suelen incluirse son deshabilitar servicios y funciones que no se utilicen y reemplazar algunas aplicaciones por versiones más seguras (**Figura 6**).

MENOR PRIVILEGIO

Este principio nos dice que para poder realizar sus tareas, un usuario solamente debe tener los **privilegios**

RECURSOS EN INGLÉS III

Security Tube (**www.securitytube.net**) es un sitio similar a **YouTube** con videos relacionados con la seguridad de la información. Contiene material interesante, como *Criptografía sobre llaves públicas* y videos graciosos, como *Instalar Vista en tan solo 2 minutos*, entre otros.

FIGURA 6.
Es recomendable configurar los servicios de Windows al instalar el sistema operativo.

mínimos necesarios para dicha tarea y el acceso a los recursos indispensables, no más. Esto trae una serie de ventajas muy interesantes. Por ejemplo, el hecho de tener menos aplicaciones y servicios corriendo disminuye la probabilidad de que se pueda explotar un error que comprometa al sistema. Por otro lado, apreciamos un incremento en el rendimiento de los sistemas y equipos, ya que se reduce la carga del procesador y la memoria. Otra ventaja es que, incluso al momento de detectarse alguna falla, realizar la depuración del sistema es más sencillo y rápido.

Un usuario solamente debe tener los privilegios mínimos necesarios para dicha tarea y el acceso a los recursos indispensables, no más

CONTROL DE CAMBIOS

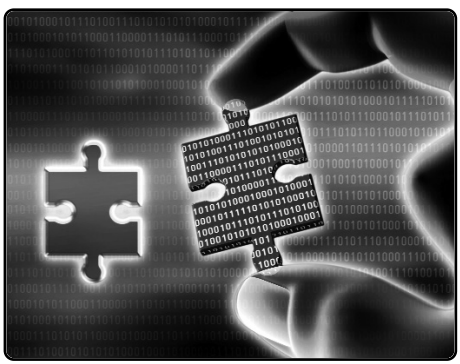
El proceso de **control de cambios** busca resguardar el modelo de seguridad de una organización de la implementación de determinadas modificaciones que puedan corromperlo. Comúnmente, un usuario pide un cambio en algún sistema que genera una posible brecha de seguridad. Puede ser la instalación de un software especial, el reemplazo de determinado hardware, la modificación de reglas en un

RECURSOS ACADÉMICOS

Algunas universidades tienen en su sitio web excelentes recursos e información para ser descargada: Universidad Politécnica de Madrid (**www.upm.es**), Universidad Politécnica de Valencia (**www.upv.es**) y Universidad Autónoma de México (**www.unam.edu.mx**), entre otras.

firewall y un largo etcétera. En términos generales, los usuarios no son conscientes de las implicancias que las modificaciones pueden tener para la seguridad de la organización. Es el responsable de seguridad de la información quien debe analizar el impacto de dichos cambios antes de implementarlos. La efectividad en los controles de cambios permite, entre otras cosas, determinar problemas como violaciones de políticas internas, fallas de hardware e infecciones por **malware**.

Respecto de las aplicaciones y al sistema operativo, el control de cambios se puede implementar en las **actualizaciones** (*upgrades*), **service packs**, **parches**, **reglas de firewall** o **proxy** y muchos elementos más. En cuanto a los dispositivos de hardware, fundamentalmente puede aplicarse a **discos** y **periféricos**, **drivers**, **BIOS** y **firmwares**, entre otros.



CONTROL DE INTEGRIDAD

Otra de las buenas prácticas es realizar **controles de integridad** sobre los archivos críticos. Esto implica obtener una pequeña firma o resumen de cada archivo, que lo represente unívocamente. Lo que permite una buena implementación de un control de integridad es identificar modificaciones indeseables en archivos críticos, que pueden ser realizadas por algún atacante, por la infección del sistema por malware, etcétera. Más adelante veremos en detalle la forma técnica de llevar a cabo dichas verificaciones, y sus vulnerabilidades.

POLÍTICAS DE CUENTAS

La definición y posterior implementación de las **políticas de cuentas** son otras de las mejores prácticas en lo que a seguridad de la información corresponde. Éstas contemplan la correcta definición de los usuarios, los recursos a los que tendrán acceso, y una política de **contraseñas** acorde a los tiempos que corren.

Por ejemplo, sería ridículo exigirle a un usuario que colocara una contraseña de 14 caracteres, combinando letras en mayúscula y minúscula, números y

EL IEEE

El *Institute of Electrical and Electronics Engineers* (**IEEE**) tiene su sitio web en **www.ieee.org**. Es una asociación técnico-profesional mundial, sin fines de lucro, dedicada a la estandarización de normas tecnológicas.

caracteres especiales, que tenga que cambiarla cada una semana y no pueda repetirse por doce períodos. De este modo, lo único que conseguiríamos es que la persona la anote en un papel para recordarla, y la medida que pretendía aumentar la seguridad termina por ser contraproducente.

REGISTROS Y LOGS

Los **registros** y **logs** de auditoría son una parte fundamental de todo esquema de seguridad. Lo que nos permite obtener un sistema de logs es un rastro de determinados eventos que se dieron en un momento determinado. Una característica de estos sistemas es que la grabación se realiza en un medio de ingreso secuencial, los datos se van almacenando sucesivamente en el área seleccionada.

Actualmente, la generación de logs no es una dificultad, prácticamente cualquier dispositivo o aplicación tiene su propio sistema. El problema asociado a esto es que una vez originada, toda esa información tiene que ser interpretada. Para ello se utilizan diversos programas que se encargan de analizar todos los registros generados, correlacionar datos y así producir nueva información, más valiosa que la anterior y en mucha menor cantidad.

El sistema para realizar las copias de seguridad también debe estar determinado

Otro punto a tener en cuenta con los sistemas de logs es su gestión. Esto comprende la selección de los eventos que se van a registrar (por ejemplo,

EL IETF

El *Internet Engineering Task Force* (**IETF**) tiene su sitio en **www.ietf.org** y es una organización internacional abierta de normalización, cuyo objetivo principal es contribuir a la ingeniería de Internet. Es la mayor autoridad para establecer modificaciones técnicas en la red.

intentos de **login fallidos**), los ciclos de rotación, la compresión, la verificación de su integridad y la protección de estos mediante cifrado (**Figura 7**).

En forma análoga a los sistemas de registros, el sistema para llevar a cabo las **copias de seguridad** también debe estar determinado. Para que este proceso de *backup* sea efectivo, los datos tienen que haber sido clasificados en un proceso anterior. Algunos ejemplos típicos de éstos son planillas de cálculo, inventarios, información de clientes, secretos comerciales, planes de investigación y desarrollo, etcétera.

Otra consideración importante es que los datos suelen cambiar más frecuentemente que el software y el hardware, por lo que los esquemas de backup deben estar acordes a dichas modificaciones. Si un dato se modifica una vez al mes, no se recomienda realizar su backup diario, ya que de otra manera se estarían desperdiciando recursos.

Como parte de la estrategia de backups, deberán existir normas claras que permitan regular, entre otros puntos, la información a resguardar, su frecuencia de operación, las personas responsables de su ejecución, la periodicidad con la que se comprobará la efectividad del sistema implementado y el lugar físico donde se almacenarán las copias generadas. Si consideramos las distintas modalidades de operación, las tres más conocidas y utilizadas son:

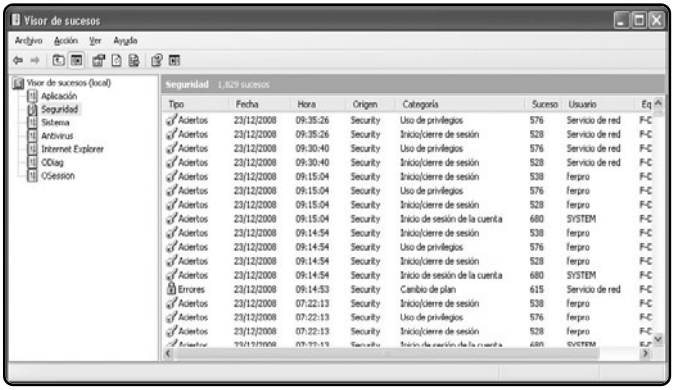
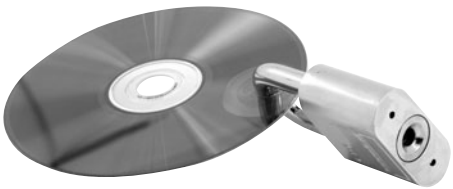


FIGURA 7.
El `Visor de sucesos` **de Windows registra todos los eventos que ocurren en el sistema.**

BUENAS PRÁCTICAS Y VULNERABILIDADES

Entre las buenas prácticas y la ética del mundo de la seguridad informática, se considera que antes de realizar un aviso público de una vulnerabilidad, el investigador debe avisar a la empresa afectada y proporcionarle los detalles sobre ésta.



- La modalidad **full** o **normal**: en ésta se copian todos los archivos seleccionados, hayan sido modificados o no, y se reestablece el atributo de archivo modificado a cero.
- La modalidad **incremental**: se copian solamente los archivos creados o modificados desde la última copia, sea ésta full o incremental. En esta modalidad, se marcan los archivos como copiados y se cambia el atributo de archivo modificado a cero.
- La modalidad **diferencial**: aquí se copian los archivos creados o modificados desde la última copia de seguridad full o incremental, pero en este caso no se marca el atributo del archivo como copiado, es decir, no se reestablece a cero. Una copia de seguridad diferencial no es tan rápida como una incremental, pero es más veloz que una completa; requiere más espacio que una incremental, pero menos que una completa.

A modo de resumen, el backup full representa el proceso de backup y recuperación de datos más simple, pero insume muchos recursos para llevarse a cabo. Si bien los backups incrementales y diferenciales son más complejos, requieren menos tiempo y recursos.

BIBLIOGRAFÍA Y REFERENCIAS

Gran parte de la información de esta sección fue obtenida de los siguientes sitios web, que cuentan con abundante contenido orientado a evitar que no se cumplan las buenas prácticas:

- **Laboratorio ESET** (http://blogs.eset-la.com/laboratorio)
- **IBM Internet Security Systems** (www.iss.net).

RESUMEN

En este capítulo, nos hemos introducido en el apasionante mundo de la seguridad informática. Hemos visto sus conceptos fundamentales, las buenas prácticas a tener en cuenta y la terminología para comprenderla.

Multiple **choice**

1 ¿Cómo se llama la modalidad de backup en que se copian solamente los archivos creados o modificados desde la última copia?

a- Full.
b- Incremental.
c- Funcional.
d- Diferencial.

2 ¿Cómo se llama la persona que finge tener conocimientos que en verdad no posee?

a- Lammer.
b- Script kiddie.
c- Newbie.
d- Phreaker.

3 ¿Qué significa, en castellano, el término crack?

a- Transformar.
b- Romper.
c- Cambiar.
d- Crear.

4 ¿Cómo se llama la persona que utiliza programas creados por terceros sin conocer su funcionamiento?

a- Lammer.
b- Script kiddie.
c- Newbie.
d- Phreaker.

5 ¿Cuál de los siguientes hacker se orienta a los servicios telefónicos?

a- Lammer.
b- Script kiddie.
c- Newbie.
d- Phreaker.

6 ¿Cuál de las siguientes no es una modalidad de backup?

a- Full.
b- Incremental.
c- Funcional.
d- Diferencial.

Respuestas: 1-b, 2-a, 3-b, 4-b, 5-d, 6-c.

Capítulo 2

Espionaje corporativo

En este capítulo, conoceremos todo sobre el espionaje, sus motivaciones, su impacto en los negocios, entre otros temas.

Espionaje corporativo

El **espionaje corporativo** existe como tal prácticamente desde la revolución industrial, donde los secretos productivos de las fábricas comenzaban a ser la clave de los negocios. Con el correr del tiempo, estos secretos fueron tomando la forma de fórmulas químicas, procesos productivos, materiales especiales, proyectos de investigación y desarrollo, y campañas publicitarias, que las empresas guardaban celosamente. En este contexto, las compañías buscaban obtener ventajas competitivas al conseguir esa valiosa información de diversas maneras. De este modo, las empresas alcanzaban una considerable superioridad respecto de sus competidores que no contaban con ella. Así nacen los espías industriales, quienes obtenían esa información, obviamente, por medio de métodos poco éticos y legales.

Contrariamente a lo que sucede con los bienes tangibles, para los cuales es sencillo darse cuenta si han sido robados, puede darse el caso de que por muchos años se le haya quitado a una empresa su **propiedad intelectual** o su ventaja competitiva y que nadie se haya dado cuenta de ello. La competencia podría lograr beneficios en el mercado constantemente, por ejemplo, al ofrecer una mejor oferta en una licitación o al desarrollar mejoras más económicas o más rápidamente a productos. Esto demuestra que los secretos corporativos en manos de la competencia implican un conocimiento que puede volverse en contra.

Debemos tener en cuenta que el espionaje corporativo no solo se limita a las grandes compañías y a las grandes inversiones. Es posible que los **espías** profesionales obtengan el perfil de una pequeña empresa a partir de sus conversaciones privadas, documentos desechados, proyectos y restos de materiales de viajes. A partir de los avances y la masificación de Internet y de las tecnologías relacionadas, es cuando esta actividad encuentra un nuevo vector.

MOTIVACIONES

Como mencionamos anteriormente, todo lo que pueda generarle beneficios a una compañía y ponerla en una posición de ventaja sobre la competencia es blanco natural del espionaje corporativo o industrial. También vimos que eso podía variar entre el código fuente de un programa, un software pronto a lanzarse, los planes de marketing, secretos corporativos, documentación de investigaciones, etcétera.

Si seguimos dejando volar nuestra imaginación, otro ejemplo práctico sería frente a una licitación pública.

Ésta suele representar grandes beneficios para la empresa que la gana: pensemos por un momento qué pasaría si la competencia obtuviera la oferta final antes de que fuera publicada. Sin dudas sería una gran pérdida de dinero.

Pero no solo nos vamos a centrar únicamente en las empresas. Por ejemplo, contemplemos por un momento una puja entre medios de comunicación, no sería descabellado, dado el contexto actual, que existieran espías que buscaran obtener detalles de las campañas, sueldos de las figuras más importantes, etcétera.

Otra motivación, también fuera del ámbito corporativo, puede ser la de conseguir información privada de personas de perfil público que pueda comprometerlas. Por medio de un viejo recurso de la retórica, muchas veces se pretende probar que una de las partes tiene razón, demostrando que la otra está equivocada. Extendamos un poco más este concepto: si se evidencia que el rival de una disputa no es una persona confiable o no posee valores éticos, la otra de las partes corre con ventaja. De ahí que muchas veces se busque hurgar en el pasado de celebridades, políticos y figuras de renombre, con tal de encontrar algún dato que pueda comprometer su imagen.

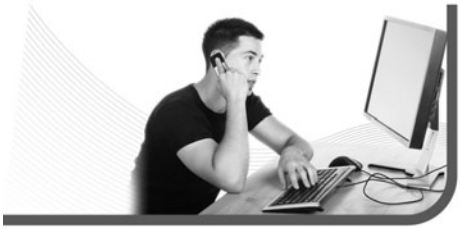
Concluimos que cualquier información **confidencial** para una organización e incluso para determinados particulares es una motivación para realizar espionaje corporativo.

ESPÍAS INDUSTRIALES

Podríamos decir que los espías existen desde que hay conflictos entre bandos. En *El arte de la guerra*, Sun Tzu destacaba su importancia de la siguiente manera: "[…] permiten al soberano sabio y al buen general golpear y conquistar mediante el conocimiento preciso de las actividades desarrolladas por el enemigo".

El espionaje corporativo existe como tal prácticamente desde la revolución industrial

Probablemente mientras estamos hablando de espías, lo primero que se nos viene a la mente son personajes de la talla de **James Bond**, **Jason Bourne** y, por qué no, **Maxwell Smart**. Pero, en realidad, en el ámbito corporativo, suele suceder que el espía no sea otro que un trabajador, y no necesariamente lo haga en forma intencional.



Un concepto clave que vamos a utilizar asiduamente en seguridad de la información es la analogía con una cadena y sus eslabones. Ésta siempre se romperá por el eslabón más débil, aquél que presente alguna falla estructural. En este caso, el eslabón más débil respecto de la protección de los datos de una organización no es otro que el mismo trabajador.

Se pueden agregar infinidad de medidas técnicas asociadas a la seguridad, pero si no está contemplado que gran parte de la seguridad depende del usuario, esas medidas no serán del todo efectivas.

Con la masificación de Internet aparecieron nuevos vectores para llevar a cabo el espionaje corporativo. El hecho de que cada vez más las computadoras estén conectadas a Internet todo el tiempo, junto a que los usuarios no son conscientes del peligro que conlleva el no tomar los recaudos mínimos de seguridad, facilita que otras personas con malas intenciones tengan acceso a información que no deberían. Aquí es donde cobra relevancia el malware o **software malicioso**.

Posteriormente, hablaremos en detalle de este tema, pero por ahora vamos a referirnos como malware a

todos aquellos programas que tengan fines perjudiciales para el dueño del sistema que está infectando. Ejemplos de esto son los **virus**, **troyanos**, **spyware**, **adware** y muchos otros especímenes.

En lo que se refiere a espionaje industrial, quizá los más perjudiciales por el impacto directo que tienen sean los troyanos y los spywares. Los troyanos, a grandes rasgos, dejan disponible al atacante una entrada al sistema, con lo cual potencialmente tiene el control sobre el equipo y sobre la información que éste aloja.

Los spywares, en cambio, son pequeños programas que recopilan información de nuestro sistema y la envían a distintos servidores para que sea analizada. Pensemos por un breve instante lo que podría suceder si la computadora de un gerente o un directivo estuviese infectada por algunos de estos programas. Potencialmente, toda la información que se encuentre dentro de ese equipo estaría al alcance del pérfido atacante (**Figura 1**).

Con la masificación de Internet, aparecieron nuevos vectores para llevar a cabo el espionaje corporativo

Volvamos al espionaje corporativo en términos generales: según datos de un cálculo estimado, aproximadamente dos tercios del total del espionaje corporativo en Estados Unidos es llevado a cabo por los propios trabajadores. En algunas ocasiones, los empleados venden secretos corporativos con fines de lucro, pero en otros casos pueden hacerlo solo por venganza.

Un empleado disconforme es capaz de enviar sus secretos corporativos directamente a la competencia. Pero como mencionamos anteriormente, puede ser

FIGURA 1.
El portal www.delitosinformaticos.com contiene noticias y leyes que ayudan a abordar la temática legal.

que la acción no sea intencional. Por ejemplo, las entrevistas de trabajo constituyen una fuente de espionaje más discreta para las compañías. Algunas preguntas hechas de la forma correcta, tales como ¿cuáles fueron tus tareas? o ¿cuál es el próximo paso de su organización?, son formuladas con el fin de conocer algunas metodologías o secretos internos de la competencia.

IMPACTO EN LOS NEGOCIOS

Sin dudas, el espionaje industrial tiene un impacto negativo en las organizaciones y las pérdidas que trae aparejadas son millonarias. El informe anual de seguridad **FBI/CSI** 2008 (*FBI/CSI Computer Crime & Security Survey 2008,* **www.gocsi.com**) refleja esta realidad con estadísticas interesantes sobre las seguridad en las empresas.

Si tenemos en cuenta que el total de organizaciones encuestadas fue de 494, incluyendo empresas, entidades gubernamentales, asociaciones, etcétera, y que el total de pérdidas ascendía en promedio a los US$ 350.000 por compañía, las cifras obligan a estar atentos a este tema.

Por otro lado, según un estudio de **ESET** y del **IBM Internet Security Systems** de fines de 2007, los malware más utilizados por los atacantes son los troyanos (28%) y los gusanos (14,8%).

Todos los ataques descriptos atentan contra la información confidencial de la organización y se puede usar por quien la obtuvo para realizar acciones de espionaje corporativo, entre otros fines maliciosos. Como también se puede ver en las estadísticas, las pérdidas asociadas son muy elevadas.

DATOS DEL INFORME DEL FBI/CSI 2008

El porcentaje de pérdidas asociadas al malware fue del 52%. Las pérdidas por gusanos, troyanos y spywares ascendieron a US$ 8.392,00. El 37% de los encuestados sufrió pérdidas dentro de sus organizaciones, mayores al 20%, a través de atacantes internos.

Sistema sin parches: problema asegurado

Es normal escuchar casi a diario sobre las nuevas actualizaciones de las aplicaciones, tanto en materia de seguridad como de funcionalidad. En ese dinámico universo de idas y venidas de software por Internet, es que nos encontramos frente a la necesidad de comprender qué es lo realmente necesario para mantenernos seguros. No debemos olvidar que un atacante será el primero en tener que contar con un sistema seguro de trabajo.

En el caso de los parches, se trata más bien de una actualización para solucionar problemas

PARCHES Y HOTFIXES

Algunos términos como **patches** (parches) o **hotfixes** (interpretado como **revisión**) son los que encontramos en el folclore de la industria del software. En pocas palabras, podemos decir que un hotfix es un componente diseñado para **reparar problemas** que ocurren en un número de equipos de trabajo relativamente pequeño. Suele ser creado por el proveedor de software cuando surgen ciertos inconvenientes de compatibilidad o de funcionalidad con un producto de un fabricante utilizado en una plataforma de hardware específica.

Los hotfixes, por lo general, no son sometidos a pruebas tan rigurosas antes de ser publicados, pues su idea es solucionar rápidamente problemas críticos, por lo tanto, de no ser necesarios, no se deberían instalar. Un atacante podría, si conoce esta recomendación, saber que no siempre está todo

APACHE, EL NOMBRE DEL PARCHE

Cuenta la leyenda digital que el servidor web más utilizado evolucionó como un conjunto de parches para el servidor **NCSA** (*National Center for Supercomputing Applications*) para añadir funcionalidades.

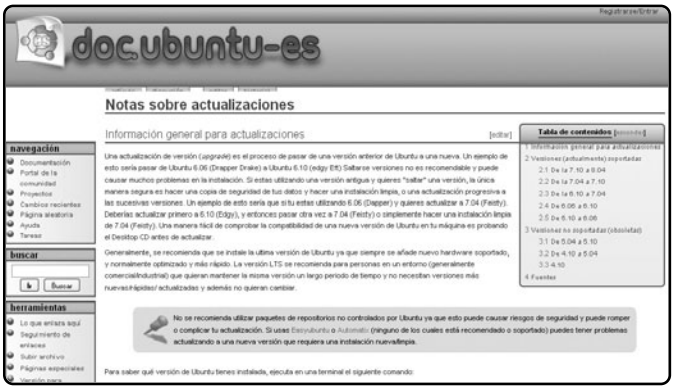


FIGURA 2. En el sitio oficial de Ubuntu en español, encontraremos notas sobre actualizaciones críticas para dicha distribución de Linux.

reparado en los equipos de su objetivo. Por supuesto que su instalación puede ser manual o automática, de acuerdo con el sistema operativo (**Figura 2**).

En el caso de los parches, se trata más bien de una **actualización** para solucionar problemas o mejorar la usabilidad de cierta aplicación. Los podemos aplicar a un binario ejecutable o al código fuente de un programa. En el caso del binario, es posible modificarlo con cambios a nivel de bits o bien reemplazarlo por completo.

Microsoft tiene una herramienta llamada **Network Security Hotfix Checker**, que sirve para realizar verificaciones de parches instalados y podemos descargarla desde **www.microsoft.com/technet/Security/tools/hfnetchk.mspx**.

SERVICE PACKS

Otro concepto de la atmósfera del software, cuyo nombre popularizó Microsoft, es el de **service pack**, que no es más que un conjunto de parches que se utiliza para actualizar, corregir y mejorar aplicaciones y sistemas operativos. Pueden ser **incrementales** (no contienen las actualizaciones anteriores) o **acumulativos** (cada uno contiene el anterior). Un atacante siempre intentará descubrir si su sistema objetivo tiene instalado un service pack, ya que esto le dirá en buena medida a qué es vulnerable. En el caso de sistemas Windows, el recurso más útil es el del propio sitio web de soporte de Microsoft: **http://support.microsoft.com/sp**.

SISTEMAS AUTOMATIZADOS DE ACTUALIZACIÓN

Muchos creadores de software diseñaron sistemas automáticos para la aplicación de parches, a fin de

resolver los posibles problemas derivados de la gran cantidad de aplicaciones existentes para ser administrados y mantenidos. El ejemplo más conocido de un sistema de aplicación de parches es el *Windows Server Update Services* (**WSUS**) de Microsoft, aunque también los hay en otras plataformas.

A los fines de un atacante, todo esto puede ser utilizado mediante una técnica especial que implique una descarga automática de parches o actualizaciones falsas. Con esto en mente, el investigador argentino Francisco Amato de **Infobyte** (**www.infobyte.com.ar**) desarrolló un conjunto de herramientas de explotación llamado **Evilgrade**, que utiliza técnicas de *man-in-the-middle* (en **DNS**, **ARP**, **DHCP**, etcétera) para tomar el control de un sistema remoto que realiza la tarea de manera no segura. El sitio **Windows Security** presenta aplicaciones de gestión de parches para plataformas Microsoft. La lista de herramientas se encuentra en **www.windowsecurity.com/software/patch-management**.

Muchos creadores de software diseñaron sistemas automáticos para la aplicación de parches

El día después: Informática Forense

Según las estadísticas, en la última década hubo más de 20.000 ataques exitosos a sitios web solamente en Argentina, y a nivel mundial los números son escalofriantes. Estos casos se transforman en el escenario de la **Informática Forense**. Una excelente definición de este término la encontramos en un texto de origen australiano: "Es la técnica de capturar, procesar e investigar información procedente de sistemas informáticos por medio de una metodología, con el fin de que pueda ser utilizada en la justicia" (Rodney McKennish, 1998).

Según la Oficina Federal de Investigación de Estados Unidos (**FBI**), la Informática Forense es: "La ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio informático".

En cuanto a los incidentes informáticos, éstos pueden ser de distinta naturaleza, como ser el robo de propiedad intelectual, el fraude, la distribución de virus, la denegación de servicio, la extorsión, la estafa, el acceso no autorizado, el robo de servicios o el abuso de privilegios.

BUG HUNTING

Se habla de *bug hunting* como el hecho de "cazar errores" de software, con el objetivo de repararlo para conseguir mejores productos de software y evitar que ocurran en adelante. Las fallas encontradas pueden ser reportardas al responsable.

DELITOS INFORMÁTICOS

Este término está muy presente en la actualidad, dadas las leyes que se promulgaron al respecto en los últimos años. Podemos afirmar que son simplemente los **actos criminales** en los cuales se encuentran involucradas las **computadoras** (**Figura 3**).

Pueden ser cometidos directamente contra las computadoras, puede que éstas sean las que contienen la evidencia, o bien ser utilizadas para cometer delitos. Debido a que nadie desea ser acusado de delincuente informático, y mucho menos terminar en la cárcel ni pagar multas, es importante saber que, así como los Estados más avanzados del mundo, varios países de Latinoamérica poseen leyes sobre el tema.

Las contravenciones penadas por estas normas abarcan acciones como ser la distribución de pornografía infantil; la interrupción, obstrucción o desvío de una comunicación; el acceso indebido a bases de datos privadas; la alteración del normal funcionamiento de un sistema; la modificación o destrucción de documentos y programas o la venta

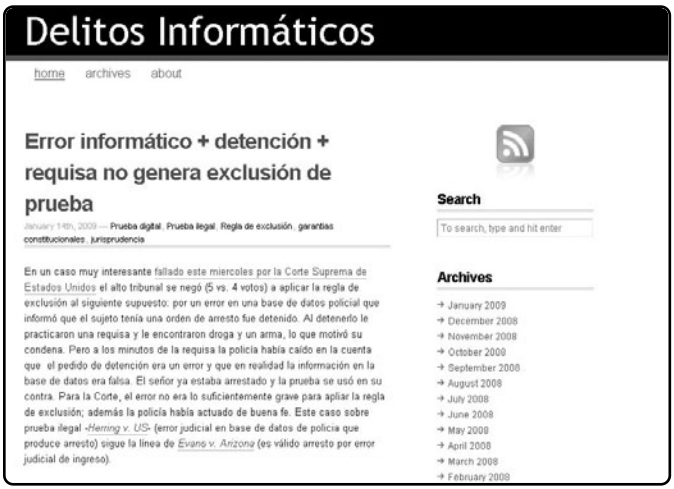


FIGURA 3.
En el blog del abogado argentino Pablo Palazzi (www.delitosinformaticos.com.ar/blog), podemos obtener información interesante y muy actualizada sobre delitos informáticos.

UNA DISCIPLINA SIN ESTÁNDARES

La Informática Forense es una ciencia relativamente nueva, que carece de estándares formales, aunque hay algunos proyectos en desarrollo, como el **Código de Prácticas para Digital Forensics** (**C4PDF**) de Roger Carhuatocto, entre otros.

y distribución de programas destinados a hacer daño en un sistema informático.

LA EVIDENCIA DIGITAL

En los sucesos de la vida real, la evidencia lo es todo respecto de la demostración, ya que se utiliza para establecer los hechos y permite relacionar diferentes eventos. La **evidencia digital**, específicamente, es un tipo de prueba física, menos tangible que otras formas de evidencia (ADN, huellas digitales, componentes de computadoras, papeles). Tiene algunas ventajas sobre su contraparte no digital porque, por ejemplo, puede ser duplicada de manera exacta, es posible detectar si ha sido alterada y, aun si es borrada, a veces recuperarla. Esto se resume en: repetible, recuperable, redundante e íntegra.

Un atacante intentará siempre destruir la evidencia, por lo que deseará conocer todos los sitios donde permanecen las copias. También tratará de generar problemas sobre la posible evidencia con su alteración, haciendo que el sistema la elimine (sobreescritura de datos en disco y memoria) o simplemente con medios más sofisticados en los investigadores.

Existe una regla muy importante en la Informática Forense, que asegura que **no siempre vale la pena investigar**. Veámoslo de la siguiente forma:

1) Se produce un incidente.
2) Se analizan las pruebas.
3) Se generan hipótesis.
4) Se presume una respuesta.

IOCE

La *International Organization On Computer Evidence* (**IOCE**) funciona desde 1995 y está compuesta por agencias gubernamentales. Realiza un foro de intercambio de información sobre investigaciones de evidencia digital y computación forense. Su sitio web es: **www.ioce.org**.

Pero... ¿hay acaso absoluta certeza de lo que se cree que ocurrió? La respuesta en general es: no. Esto ocurre debido al mismo problema que siempre tenemos en la seguridad, los "buenos" corren detrás de los "malos" y, por lo tanto, estos últimos llevan ventaja.

Pero desde un punto de vista más práctico, investigar implica un consumo de tiempo, esfuerzo, dinero y recursos humanos, puestos a disposición del caso, e incluso muchas veces se produce la inutilización del material para analizar, lo que en ocasiones puede reducir la productividad de los damnificados. Por ejemplo, si un atacante accede a un servidor de una empresa y toma control de éste, tal vez el investigador necesite sacar de producción dicho equipo para investigarlo en detalle, lo cual dejaría a la empresa sin ese servidor. Aquí la decisión será más bien gerencial: ¿perder productividad a fin de intentar detectar al atacante?, ¿tiene la empresa una política ante incidentes?, ¿se debe continuar investigando o no?

Un buen investigador sabrá por experiencia cuándo ya no es conveniente seguir avanzando. Según especialistas del FBI, un incidente de 1 hora de duración puede insumir, en promedio, unas veinte horas de análisis.

Un atacante entonces sabrá muy bien que los investigadores tienen un límite y actuará con la consideración de que, llegado el caso, ya nadie intentará

LAS CUATRO REGLAS

Citaremos cuatro reglas mencionadas en el texto **A las puertas de una nueva especialización**, referido a Informática Forense: **1)** minimizar el manejo del original; **2)** documentar los cambios; **3)** cumplir con las reglas de la evidencia y **4)** no exceder el conocimiento propio.

continuar siguiendo sus rastros. En ese punto, sin ser el crimen perfecto, habrá ganado.

RESPUESTA A INCIDENTES

Para hacer frente a los incidentes de manera inmediata, se suele contar con el apoyo de los *Computer Security Incident Response Teams* (**CSIRT**) o **Equipos de Respuesta a Incidentes de Seguridad** que son, en palabras de la gente de **ArCERT**, el CSIRT de Argentina: "Organizaciones responsables de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad". Generalmente sus servicios son prestados para un área de cobertura definida que podría ser una entidad relacionada u organización de la cual depende, una corporación, una organización de gobierno o educativa, una región o un país, una red de investigación o un servicio pago para un cliente. Un ataque tendrá consecuencias más graves en caso de que la organización no cuente con un plan de respuesta ante incidentes (**Figura 4**).

FIGURA 4.
ArCERT fue creado en 1999 y se encarga de difundir información con el fin de neutralizar incidentes en forma preventiva o correctiva.

RECURSOS DE CERT ONLINE

Cada país suele tener su propio CERT o equipos de respuesta a incidentes. Aquí mencionamos algunos de ellos: CERT® (**www.cert.org**), ArCERT (**www.arcert.gov.ar**), US-CERT (**www.us-cert.gov**), UNAM CERT (**www.cert.org.mx**) y CERT Chile (**http://www.clcert.cl**).

TEORÍA ANTIFORENSE

Así como existen técnicas que sirven para determinar la reconstrucción de hechos y la elaboración de teorías sobre ataques e incidentes, también hay prácticas que tienen como objetivo dificultar dicho proceso. Estas técnicas, denominadas **antiforenses**, suponen el conocimiento absoluto de la manera en que un investigador aplicará sus conocimientos para buscar información y confeccionar teorías. De esta forma, al saber qué es lo que se hará para descubrir un rastro, se puede tener en cuenta una forma especial de ocultarlo para que no salga a la luz en un análisis.

En un nivel más profundo de estudio, las técnicas antiforenses pueden ser derrotadas con medidas **antiantiforenses**, es decir, conocer el accionar y las técnicas antiforenses y tomar medidas tales que faciliten cumplir los objetivos del análisis inicial.

REPORTES DE INVESTIGACIÓN

Un gran trabajo de investigación podría fallar en su momento cúlmine, y los investigadores tienen muy en cuenta esto al finalizar su tarea. En pocas palabras, no solo es importante descubrir qué ocurrió, sino también que los demás lo comprendan. Esta realidad determina al menos dos niveles de discurso, uno más bien técnico y otro más bien gerencial. Esto es más importante aun cuando se trata de un proceso legal, ya que los peritajes deben cumplir con determinadas normas que no se habrán de evitar.

Normalmente, la presentación de los resultados se hará a una empresa, a los abogados, a la corte, o bien al individuo que lo solicite. La aceptación de ésta, en cualquier caso, dependerá de diversos factores, como ser la forma de presentación, los antecedentes y calificaciones de la persona que realizó el

En un nivel más profundo de estudio, las técnicas antiforenses pueden ser derrotadas con medidas antiantiforenses

CUESTIONES TÉCNICAS Y LEGALES

Para realizar un adecuado análisis informático forense se requiere un equipo multidisciplinario que incluya profesionales expertos en derecho tecnológico y expertos técnicos en metodología forense; para garantizar el cumplimiento de los requerimientos jurídicos y técnicos.

análisis y la credibilidad del proceso que fue utilizado para la preservación y el análisis de la evidencia.

Informe ejecutivo

Un **informe ejecutivo** contiene mayormente las conclusiones del caso, sin incorporar detalles técnicos, dado que las personas que lo reciben finalmente no son, por lo general, especialistas. Pueden estar acompañados por imágenes aclaratorias, diagramas de flujo, líneas de tiempo, etcétera. Muchas veces incluyen un análisis de costos y valor de las pérdidas sufridas por el incidente. Por supuesto, también contienen las posibles hipótesis sobre el caso.

Informe técnico

Para el caso del **informe técnico**, el detalle a nivel informático es mucho mayor, ya que reflejará la metodología empleada y, en gran parte, las habilidades del investigador. En éstos, podemos encontrar resultados de pruebas sobre software y los datos, capturas de protocolos, etcétera. Este informe indicará técnicamente por qué la conclusión sacada por el investigador es tal y no otra.

METODOLOGÍA DE INVESTIGACIÓN

Las metodologías nos aseguran que los procesos llevados a cabo puedan ser repetibles de manera sistemática. En este caso, el proceso se realiza sobre la evidencia digital de una forma legalmente aceptable y siguiendo determinados pasos:

- **Identificación**: es el primer paso en el proceso. Si sabemos qué evidencia está presente, dónde y cómo se guarda, determinamos los procesos para su recuperación. La evidencia puede extenderse a cualquier dispositivo electrónico capaz de almacenar información. Debemos poder identificar el tipo de información y el formato en que se guarda, para usar la tecnología apropiada para extraerlo.
- **Preservación**: es indispensable que cualquier examen de los datos se lleve a cabo de la manera menos intrusiva posible. Hay circunstancias donde los cambios de datos son inevitables, pero debemos hacerlo en la menor medida posible. La alteración de todo lo que tenga valor de evidencia debe ser registrada y justificada.

LECTURAS RECOMENDADAS

Informática forense liderando las investigaciones (Jeimy J. Cano), Credenciales para investigadores forenses en informática: **www.virusprot.com/Col8.html** y *Evidencia digital, normas y principios* (FBI): **www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm**.

- **Análisis**: comprende la extracción, el procesamiento y la interpretación de los datos digitales. Una vez obtenida la evidencia, requiere de un proceso de estudio antes de que pueda ser comprendida.
- **Presentación**: incluye la manera formal de la presentación, la especialización y las calificaciones del perito. Contempla la credibilidad de los procesos empleados para producir la evidencia que se está presentando ante quien juzga.

Durante todo el proceso será fundamental conservar lo que se denomina **cadena de custodia**, es decir, todas las manos por las que pasa la evidencia y qué procesos sigue mientras se trabaja con ella. Un atacante que pueda alterar la cadena de custodia podría obtener acceso a la implantación de falsas pruebas y modificar la evidencia. El atacante y el investigador estarán enfrentados en lo referido a la Informática Forense, y el que posea mayores conocimientos sobre determinados temas, tendrá mejores posibilidades de cumplir con su objetivo.

Todo medio utilizado para transportar información digital puede contener evidencia

Ambos deberán conocer en profundidad cómo la evidencia es creada y cómo se puede **falsificar**.

Medios digitales de almacenamiento

Todo medio utilizado para transportar información digital puede contener evidencia (**Figura 5**). Entre éstos, se encuentran discos duros (aún algunos disquetes), CD/DVD, tape backups, dispositivos USB y tarjetas de memoria (SD, XD, etcétera).

MÁS LECTURAS RECOMENDADAS

A las puertas de una nueva especialización: la informática forense (Alberto David Airala, Osvaldo Horacio Rapetti): **www.upcndigital.org/advf/documentos/447b111c79fe4.doc** y *Metodología de análisis forense informático* (Julio Ardita, 2007).

Una de las mejores habilidades de un atacante será tener conocimiento sobre la forma en que se almacena la información en los distintos medios, los sistemas de archivos asociados y sus formatos, y estar familiarizado con los estándares existentes. De esta manera, conocer el formato **ISO 9660**, el **UDF** o los distintos sistemas de archivo, como **ext3**, **NTFS**, **FAT32**, ofrecerá ventajas a la hora de atacar un objetivo determinado con características propias. También ayudará el hecho de tener conocimientos sobre electrónica y hardware, y por qué no, algo de física y matemática.

Recopilación de la información

Las ubicaciones posibles de los datos a analizar podrán ser tan diversas como la informática en sí misma. Por ejemplo, la PC origen del Intruso seguramente contendrá información valiosa, así como también el sistema de acceso (conexión) a las redes internas, la PC de la víctima, y eventualmente, la PC que se utilizó para lanzar el ataque, que no necesariamente será la misma desde donde se origina.

Para el caso de los dispositivos electrónicos, se requiere una comprensión completa de la estructura física y del funcionamiento de los medios de almacenamiento, así como la forma y la estructura lógica del modo de archivar los datos allí. La complejidad se simplifica con herramientas de recuperación adecuadas, ya que mucho del conocimiento exigido se integra en el software de relevamiento y la recuperación de datos.

También nos referimos a cualquier dispositivo capaz de guardar información, que posea tanto valor como evidencia: celulares, PDA, routers, etcétera. En este caso, la estandarización de dispositivos ha permitido que la extracción de datos sea más fácil y que se pueda realizar la recuperación en dispositivos específicos.

Muchas veces los atacantes cuentan con mayor nivel tecnológico que los propios investigadores, por lo que es posible que éstos no puedan recuperar los datos o analizar las evidencias que dejó un incidente.

FIGURA 5.
Un error de seguridad es encontrar un pen-drive perdido y conectarlo al propio equipo para ver su contenido.

RESUMEN

En este capítulo, estudiamos la realidad del espionaje corporativo, sus motivaciones y su impacto en los negocios. Además, hemos analizado los aspectos más importantes de la Informática Forense, una ciencia en pleno desarrollo.

Multiple **choice**

1 **¿Desde qué época existe el espionaje corporativo?**
a- La década del ochenta.
b- La Revolución Industrial.
c- La Segunda Guerra Mundial.
d- Las cruzadas.

2 **¿Cuál es el primero de los pasos de la metodología?**
a- Presentación.
b- Análisis.
c- Identificación.
d- Preservación.

3 **¿Cómo se llaman las técnicas que dificultan la reconstrucción de hechos y la elaboración de teorías sobre ataques e incidentes?**
a- Forenses.
b- Antiforenses.
c- Espionaje.
d- Ninguna de las anteriores.

4 **¿Cómo se llama el paso que comprende la extracción, el procesamiento y la interpretación de los datos digitales?**
a- Presentación.
b- Análisis.
c- Identificación.
d- Preservación.

5 **¿Cuál de las siguientes características pertenece a un informe técnico?**
a- Refleja la metodología utilizada.
b- Incluye un análisis de costos.
c- Contiene las posibles hipótesis del caso.
d- No incorpora detalles técnicos.

6 **¿Qué se debe conservar durante el proceso sobre la evidencia digital?**
a- La presentación.
b- El análisis.
c- La cadena de custodia.
d- El informe técnico.

Respuestas: 1-a, 2-c, 3-b, 4-b, 5-a, 6-c.

Capítulo 3
Ethical Hacking

Estudiaremos qué es un Ethical Hacker e introduciremos el concepto de los códigos de ética.

Ethical **Hacking**

En el presente capítulo, se definirán varios conceptos que servirán como base para comprender futuras secciones. Se describirá el perfil de los profesionales y se analizarán los distintos tipos de evaluaciones que se realizan actualmente.

Fundamentos

Aplicaremos un nuevo compuesto de palabras, Ethical Hacker (**hacker ético**), a los profesionales de la seguridad de la información que utilizan sus conocimientos de hacking con fines defensivos. Y si bien es cierto que los malos también se defienden, esa discusión queda sobre el tapete para ser juzgada con la escala de valores de cada uno. La función del Ethical Hacker será, por ende, determinar lo que un intruso puede hacer sobre un sistema y la información, y velar por su protección.

PERFIL DE CONOCIMIENTOS

Cualquier persona que haya tenido la suerte de conocer a un verdadero Ethical Hacker, probablemente lo primero que haya sentido es una cuota de admiración, ya sea por lo que saben, por lo que hacen, por sus valores o, tal vez, por la mera posibilidad de trabajar en algo tan apasionante.

Un Ethical Hacker será, seguramente, un experto en informática y sistemas, tendrá certeros conocimientos sobre los sistemas operativos, sabrá sobre hardware, electrónica, redes, telecomunicaciones y también programación en lenguajes de alto y bajo nivel.

Un Ethical Hacker será, seguramente, un experto en informática y sistemas

EL ORIGEN DEL TÉRMINO ÉTICA

El término ética proviene del griego **ethikos** y su significado es **carácter**. Tiene como objetos de estudio la moral y la acción humana, y se remonta a los orígenes de la filosofía moral. Una doctrina ética elabora y verifica afirmaciones y juicios en términos de malo/bueno.

Además, entenderá sobre problemas relacionados con seguridad en temáticas tales como la criptografía, los sistemas de control de acceso, las aplicaciones, la seguridad física y la seguridad administrativa (**Figura 1**).

Un Ethical Hacker seguirá un estricto código de conducta, dado que de eso se trata la primera parte del concepto (**Figura 2**). Pero no todo acaba aquí, el perfil no es una cosa estática y maciza, sino que requiere de la constante renovación en busca de nuevos conocimientos, mucha investigación, prueba de herramientas, etcétera. Por si fuera poco, quien quiera alcanzar dicho nivel, además de dedicar el tiempo suficiente, deberá armarse de un alto grado de paciencia, perseverancia, y por sobre todo, una gran dosis de humildad.

Tipos **de ataque**

Como es de suponer, no todos los ataques son de la misma naturaleza. De hecho, en este caso, nos referiremos solamente a una clasificación particular desde el punto de vista técnico. En los sucesivos capítulos, abordaremos en detalle otras clasificaciones y métodos. En esta sección, veremos los ataques al sistema operativo, a las aplicaciones, a las configuraciones y a los protocolos.

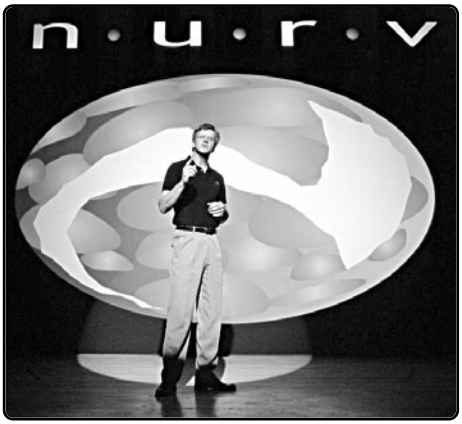


FIGURA 1. Antitrust es una película donde el hacking ético se utiliza todo el tiempo para adueñarse de la gloria. Cualquier semejanza con la realidad es pura coincidencia.

LA PALABRA HACKER EN INTERNET

Si buscamos en Internet, el término hacker arroja más de 180 millones de resultados en el buscador **Google** (que superó el billón de sitios indexados a mediados de 2008), más de 230 millones en **Yahoo!** y más de 170 millones en **Microsoft Live Search**.

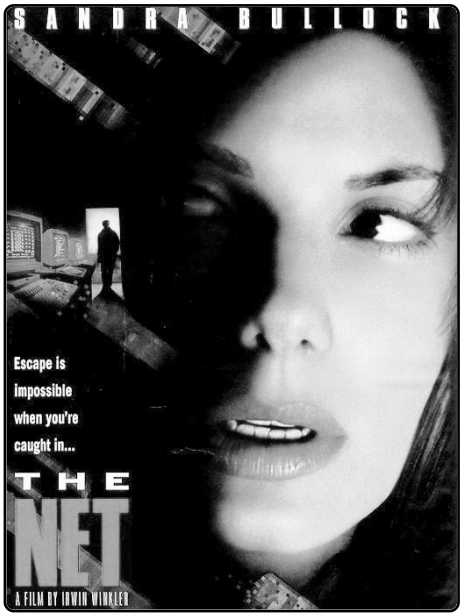


FIGURA 2. Portada del film La red con Sandra Bullock. Aborda la temática de los sistemas de seguridad y el robo de información.

ATAQUES AL SISTEMA OPERATIVO

Los ataques al sistema operativo constituyen un clásico de la seguridad. Desde esta perspectiva, la búsqueda de fallas se realizará en lo concerniente al propio sistema base de todo el resto del software, de tal forma que muchas veces, independientemente de lo que se encuentre por encima, se podrá explotar y tomar control del sistema en el caso que sea vulnerable. En última instancia, éste es el objetivo máximo al que aspira un atacante.

Así, tendremos dos líneas principales, que por supuesto serán los sistemas del tipo **Windows** y los sistemas del tipo **Linux** y derivados de **UNIX**. En el caso de los primeros, desde su origen fueron objeto de ataque dada su masificación y la relativa simplicidad con que se pudo acceder históricamente al núcleo del sistema, incluso sin contar con su código fuente. Para el caso de Linux, la situación es tal vez peor, ya que al poseer el código fuente es posible detectar problemas también a nivel de código. Pese a lo que se cree, la estadística de cantidad de vulnerabilidades de Windows no supera anualmente la de Linux, muchas veces, más bien la diferencia ha sido la velocidad con la que aparecían las soluciones en cada caso, con Linux en la delantera.

Un error en el sistema base, por tanto, hace que todo el resto tiemble. Si imaginamos por un momento un error en una librería del sistema (cualquiera sea el sistema operativo) que es utilizada por incontables aplicaciones, este fallo radical afecta directamente a todo programa que haga

PELÍCULAS SOBRE TEMÁTICAS HACKERS

La pantalla grande tuvo muchos films con temáticas hackers o del *underground* informático. Algunas de ellas son **Tron** (1982), **Wargames** (1983), **Sneakers** (1992), **The Net** (1995), **Hackers** (1995), **Pirates of Silicon Valley** (1999), **The Matrix** (1999) y **Takedown** (2000).

uso de dicha librería. He aquí la gravedad de la situación. Los ataques al sistema operativo también incluyen las implementaciones que éste realiza de las distintas tecnologías, lo cual puede incluir librerías (que deberíamos llamar **bibliotecas** en rigor de verdad). Por ejemplo, podría ser que un sistema tenga un fallo en la implementación de cierta tecnología de cifrado, lo cual haga que el cifrado sea débil, sin que se trate de un problema en el propio algoritmo de cifrado ni en la aplicación que lo utilice.

Estos ataques, que podrán ser locales o remotos, serán entonces una pieza clave en la búsqueda de errores para el intento de acceso a un sistema o red.

ATAQUES A LAS APLICACIONES

Aquí, la variedad es mayor. Existen miles y miles de piezas de software y programas de todo tipo y tamaño, disponibles en el mundo. Por supuesto, entre tantos millones de líneas de código, se producen necesariamente errores. Para los ataques a las aplicaciones, también se tendrá en cuenta lo masivo del uso. Esto implica que un programa manejado por millones de personas para leer archivos del tipo **PDF**

CLASIFICACIÓN DEL NIST

El NIST realiza una clasificación particular sobre los pentest, el **Blue Teaming Test** y el **Red Teaming Test**. El primero, con el conocimiento del personal de tecnología de la organización y el segundo, sin éste, pero con autorización de la alta gerencia.

será mejor objetivo que uno que usan unos pocos para editar cierto tipo de archivos específicos de un formato menos conocido y utilizado.

Las aplicaciones amplían, entonces, la superficie de ataque de un sistema, por lo que se recomienda siempre evitar la instalación de aplicaciones que no se requieran, y seguir el principio de seguridad que sugiere el minimalismo (**Figura 3**).

La idea de atacar la implementación de algo en lugar del software en sí mismo, también aplica para este caso. Muchos son los programas que realizan las mismas funciones, solo que algunos podrían hacerlo de forma tal que pudieran encontrarse fallos en dicha operatoria, y se comprometiera así el software, y con éste el sistema completo.

Justamente ésta es otra de las problemáticas. De acuerdo con los privilegios con los cuales se ejecute un cierto programa, si es comprometido podría afectar de forma directa al sistema, ya que se utilizaría el mismo nivel de permisos para atacarlo desde adentro, y tal vez hasta escalar privilegios para llegar al máximo nivel, lo cual se analizará posteriormente.

ERRORES EN CONFIGURACIONES

El caso de las configuraciones, ya sean del sistema operativo o de las aplicaciones, también constituyen un punto sensible, dado que por más seguro que sea un software, una mala configuración puede tornarlo tan maleable como un papel. Pensemos en un ejemplo muy elemental como sería un antivirus: la configuración deficiente podría hacer que cumpla de manera

PROGRAMACIÓN SEGURA

Es una rama de la programación que estudia la seguridad del código fuente de un software, y cuyo objetivo es encontrar y solucionar sus errores. Incluye la utilización de funciones seguras para protegerlo de desbordamientos, control del flujo y testeos en ejecución.

FIGURA 3.
Se desarrollaron programas que usaban el protocolo de ICQ para acceder a otras computadoras de manera remota.

poco efectiva su función y provoque que una buena herramienta termine por traducirse en una mala solución, por ende, en una brecha de seguridad. Aquí reside el peligro, ni siquiera las herramientas de protección y seguridad son fiables en sí mismas solo por su función. Esto podría producir algo muy grave pero normal, que es una falsa sensación de seguridad, tal vez el peor de nuestros males.

Un atacante aprovechará las configuraciones estándares de muchas aplicaciones, equipos informáticos, dispositivos de red, etcétera para utilizarlos como vía de entrada. Por ejemplo, si un programa se instala con ciertas credenciales de acceso por defecto y éstas no son modificadas, cualquiera que quiera acceder y las conozca puede hacerlo. Podríamos decir que gran parte de los problemas que se encuentran en el mundo de los sistemas se debe a errores en las configuraciones. Un sistema bien configurado es mucho menos susceptible de ser vulnerado que uno que no lo está, sin duda. Para paliar esto, se aplican las técnicas de **hardening**, las cuales veremos posteriormente.

Las configuraciones, ya sean del sistema operativo o de las aplicaciones, también constituyen un punto sensible

ESTÁNDARES INTERNACIONALES

Mencionamos algunos de los estándares internacionales asociados a la seguridad más reconocidos, y sus correspondientes enlaces: **ISO 27001** (**www.iso.org/iso**), **SoX** (*Sarbanes-Oxley*, **www.sarbanes-oxley.com**), **COBIT** (**www.isaca.org/cobit**) y **BASILEA II** (**www.bis.org/bcbs**).

ERRORES EN PROTOCOLOS

Otro gran problema al que podemos enfrentarnos es que se encuentren errores en protocolos. Esto implica que, sin importar la implementación, el sistema operativo, ni la configuración, algo que se componga de dicho protocolo podrá ser afectado.

El ejemplo más clásico de todos es tal vez el del Transmission Control Protocol/ Internet Protocol (**TCP/IP**), una suite de protocolos tan efectiva y flexible, que, luego de más de tres décadas de existencia aún perdura y continúa siendo usada. El problema aquí es que en su momento, a principios de los años 70, su diseño no obedecía a aspectos de seguridad, por determinados motivos propios de su objetivo de utilización, y con toda razón. En lo sucesivo, su uso se extendió a tal punto que comenzó a ser implementado de maneras que el propio esquema permitía, pero para fines que no había sido pensado inicialmente y transformándose, entonces, en una verdadera arma de doble filo.

De todas maneras, este es solo un ejemplo, pero no constituye un verdadero error ya que, como se dijo, su diseño es altamente efectivo, a tal punto que el modelo de referencia Open System Interconnection (**OSI**) se basó en él (**Figura 4**). Dado que existen centenares de protocolos, mayormente para ser utilizados en redes de telecomunicaciones, hay a la vez muchas posibilidades de encontrar fallos.

EL ABUELO DE LOS PROTOCOLOS

La familia de protocolos de Internet es un conjunto de protocolos que permite la transmisión de datos entre redes. Se lo denomina **TCP/IP** en referencia a sus dos protocolos más importantes. Fue desarrollado en 1972 por el **DoD** y se ejecutó en la red **ARPANET** en 1983.

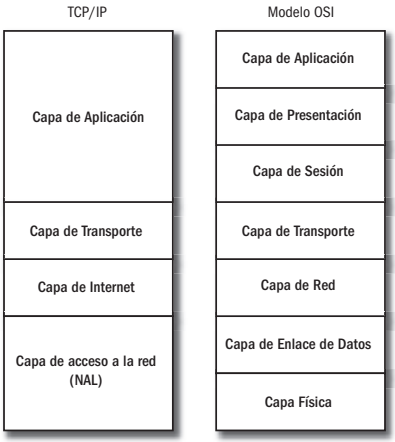


FIGURA 4. Comparativa entre la pila TCP/IP y el modelo OSI.

El problema más grave es que un error en el diseño de un protocolo implica situaciones potencialmente incorregibles, y deben realizarse modificaciones a distintos niveles para lograr resolverlo, incluso, a veces, su variación total o parcial, o su reemplazo por otro más seguro. Dentro de esta rama de errores, también incluimos los protocolos y algoritmos criptográficos, que, como veremos, tienen un alto nivel de complejidad y pueden producir huecos de seguridad realmente muy grandes, dada la función justamente de protección para la que son utilizados.

La evaluación de seguridad

En esta sección, vamos a analizar las distintas opciones al momento de evaluar la seguridad de una organización. En función de la profundidad y el alcance que se le quiera dar a dicha evaluación, se escogerá la mejor opción disponible. Así, vamos a definir los conceptos de **Vulnerability Assessment** y **Penetration Test** para sumarlos al de Ethical Hacking, previamente analizado. También veremos algunas clasificaciones en función de los distintos tipos de análisis, algunas consideraciones relacionadas con la decisión de realizar una evaluación de seguridad en una organización y cómo llevarla adelante.

Es importante mencionar que ninguna evaluación vinculada con tareas de auditoría de seguridad

Otro gran problema al que podemos enfrentarnos es que se encuentren errores en protocolos

ORGANIZACIONES ASOCIADAS AL AMBIENTE DE LA SEGURIDAD

Mencionamos varias organizaciones importantes relacionadas con el ambiente de la seguridad de la información: **ISSA** (**www.issa.org**), **ISACA** (**www.isaca.org**), **SANS** (**www.sans.org**), **EC-Council** (**www.eccouncil.org**), **ISC2** (**www.isc2.org**) y **CompTIA** (**www.comptia.org**).

(en especial las de los servicios de Penetration Test y/o Ethical Hacking) debería ser iniciada hasta que no se haya firmado un acuerdo legal que brinde a aquellos involucrados en el proyecto, expresa autorización para llevarla a cabo.

En muchos países que poseen legislación relativa a los delitos de seguridad de la información, el hacking de redes o sistemas sin previo permiso y autorización por parte de personal legalmente válido para otorgarlos es considerado un crimen.

Particularmente la ley norteamericana, en el *Cyber Security Enhancement Act of 2002,* dispone aplicar cadena perpetua a hackers que imprudentemente pongan en peligro la vida de los demás. Los hackers maliciosos que ataquen redes y sistemas informáticos relacionados con sistemas de transporte, compañías de energía o cualquier otro servicio público y generen algún tipo de amenaza contra la vida podrían ser procesados por esta ley.

Antes de continuar, vale la pena una aclaración. Respecto de la diversidad de criterios en cuanto a la definición de Penetration Test, análogamente al caso de Ethical Hacker, vamos a comenzar por decir qué no es. *Penetration Test* (o **PenTest**) no es una auditoría de seguridad, donde se evalúa hasta qué punto están bien implementadas ciertas medidas, comúnmente alineadas con alguna norma o estándar. No es un análisis de riesgo en el cual, en función de los activos de la organización, se analiza cuál sería el impacto que tendrían las distintas amenazas respecto de ellos. Tampoco es un Vulnerability Assessment. De aquí probablemente surja una duda razonable: ¿qué es un Vulnerability Assessment? A continuación, vamos a aclarar este punto.

VULNERABILITY ASSESSMENT

El concepto de Vulnerability Assessment (**VA**) o **evaluación de vulnerabilidades** es utilizado en un sinfín de disciplinas y se refiere a la búsqueda de debilidades en distintos tipos de sistemas.

ETAPAS DE EVALUACIÓN SEGÚN OVAL

1) Recoger información asociada a vulnerabilidades conocidas que afecten los sistemas de información, 2) analizar el sistema y determinar su estado en funcion de esas vulnerabilidades y si están o no presentes y 3) reportar mediante informes los resultados de dicha evaluación.

En este sentido, no solo se remite a las tecnologías informáticas a las telecomunicaciones, sino que incluye áreas como, por ejemplo, sistemas de transporte, sistema de distribución de energía y de agua, procesos de biotecnología, energía nuclear, etcétera. De esta manera, se busca determinar las amenazas, agentes de amenaza y vulnerabilidades a los que está expuesto el sistema en su conjunto. Estas debilidades usualmente refieren a todas aquéllas de carácter técnico que dependen de las cualidades intrínsecas del sistema que se esté evaluando.

En nuestro caso, teniendo en cuenta lo antedicho, vamos a hablar de Vulnerability Assessment cuando nos refiramos a un análisis técnico sobre las debilidades de una infraestructura informática y de telecomunicaciones. Puntualmente, se analizarán vulnerabilidades asociadas a distintos servidores, redes, sistemas operativos, aplicaciones y un largo etcétera vinculado a todas aquellas deficiencias técnicas (**Figura 5**).

Con relación a esto, se desarrolló el *Open Vulnerability and Assessment Language* (**OVAL**), un estándar internacional de seguridad de la información abierto cuyo

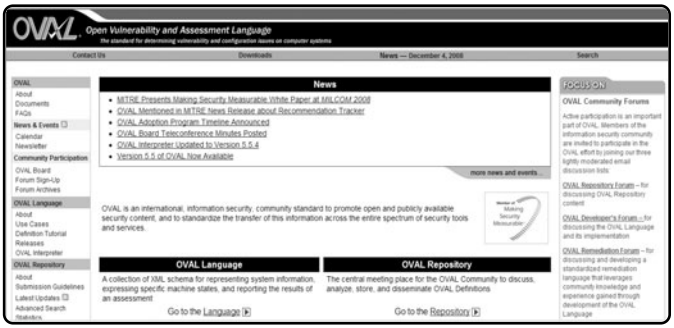


FIGURA 5.
Sitio web del Open Vulnerability and Assessment Language.

CERTIFICACIONES DE SEGURIDAD Y ORGANIZACIONES

Certified Information Systems Security Professional (**CISSP**): ISC2, *Certified Information Systems Auditor* (**CISA**): ISACA, *GIAC Certified Incident Handler* (**GCIH**): SANS y *Certified Information Security Manager* (**CISM**): ISC2.

objetivo es promocionar y publicar contenido de seguridad, y normalizar la transferencia de éste por todo el espectro de herramientas y servicios de seguridad. Incluye un lenguaje desarrollado en **XML**, utilizado para codificar los detalles de los sistemas, y una colección de contenido relacionado alojado en distintos repositorios, mantenidos por la comunidad OVAL. Su sitio es: **http://oval.mitre.org**.

PENETRATION TEST

Si extendemos el concepto de Vulnerability Assessment y nos centramos en los procesos vinculados con la información de una organización, nos acercamos a la idea de Penetration Testing. En este caso, además de las debilidades de base tecnológica, se analizarán otras cuestiones.

Por ejemplo, el uso de técnicas de ingeniería social a empleados, y búsqueda de información de la organización en forma online (a través de recursos de Internet) y *offline* (a través de medios que no tengan que ver directamente con la información publicada en la red, como las páginas amarillas, las guías de la industria, etcétera). Por lo tanto, este tipo de análisis se acerca al proceso que llevaría adelante un atacante real, de ahí su importancia.

Por lo tanto, una aproximación para definir un Penetration Test podría ser un método utilizado para evaluar el nivel de seguridad de una organización, donde quien realiza dicha evaluación simula ser un atacante real que aplica una diversa variedad de técnicas y cuyo objetivo es encontrar vulnerabilidades (conocidas o no) a partir de falencias en las configuraciones de los equipos o bien en distintos procesos o contramedidas, sean estos de índole técnica o no.

Contamos con varias fuentes de documentación para investigar sobre pentesting

BIBLIOGRAFÍA Y GUÍAS DE ESTUDIO

Algunos libros imperdibles sobre la temática de seguridad orientada a la certificación CISSP son: *CISSP All-in-One Exam* Guide - Shon Harris (McGraw-Hill), *Official (ISC)2 Guide* - Susan Hansche (Auerbach) y *The CISSP Prep Guide* - Ronald Krutz, Russell Dean Vines (Wiley).

FIGURA 6.
Sitio web de la Computer Security Division del NIST.

El *National Institute of Standards and Technologies* norteamericano (**NIST**) publicó un documento denominado *NIST Special Publication 800-115* donde se establece una guía técnica para llevar adelante un análisis y evaluación de la seguridad de la información de una organización (**Figura 6**). Por otro lado, del mismo modo que las definiciones de Penetration Test divergen, también lo hacen las etapas que comprende. La siguiente es, posiblemente, una clasificación creada en base a criterios personales en función de la experiencia y debates con colegas, aunque siempre apoyada en metodologías internacionales, de ser posible abiertas.

1) Fase de reconocimiento.
2) Fase de escaneo.
3) Fase de enumeración de un sistema.
4) Fase de ingreso al sistema.
5) Fase de mantenimiento del acceso.

CERTIFICACIONES RELACIONADAS AL PENETRATION TESTING

Algunas de las certificaciones relacionadas al pentest son: *Offensive Security Certified Professional* (**OSCP**):**www.offensive-security.com** y *GIAC Certified Penetration Tester* (**GPEN**): **www.giac.org/certifications/security/gpen.php**.

Es importante mencionar que contamos con varias fuentes de documentación para investigar sobre **pentesting**. También existen varias normas y metodologías que marcan algunas pautas y prácticas para llevar a cabo este tipo de análisis. Entre las más utilizadas, podemos destacar a la ya mencionada NIST Special Publication 800-115, la Open Source Security Testing Methodology Manual (**OSSTMM**) de **ISECOM** (**Figura 7**), y la Information Systems Security Assessment Framework (**ISAFF**) de **OISSG**.

AUTOTESTEO Y CONTRATACIÓN

Una duda que puede surgir a partir de lo visto anteriormente podría ser: ¿con qué necesidad, a partir de toda la documentación y los estándares que existen, las empresas contratan servicios externos para realizar las evaluaciones de seguridad, en lugar de hacerlo con personal propio? A continuación, iremos develando algunos puntos importantes respecto de esta inquietud. Por un lado, no todas las organizaciones poseen

FIGURA 7.
El OSSTMM es un manual de metodologías de evaluaciones de seguridad desarrollado por ISECOM.

ISECOM

ISECOM es una comunidad de colaboración e investigación en seguridad, creado en enero de 2001. El objetivo es proporcionar información. El Consejo de Administración está formado por seis países que representan a miles de miembros y voluntarios de todo el mundo.

personal especializado que esté en condiciones de realizar este tipo de evaluaciones.

En algunos casos, solo se cuenta con personal de sistemas o tecnología, que además lleva a cabo algunas tareas de seguridad, pero porque algún empleado de esa área es **el que sabe de seguridad**. Esta persona, por lo general, posee conocimientos básicos en materia de seguridad de la información, por lo que sería impensado que pueda llevar adelante un proyecto de evaluación de tal magnitud.

Por otro lado, aunque se disponga de personal idóneo para realizar dichas evaluaciones, la mayoría de las veces ésta queda sesgada por la subjetividad de quienes la hacen. Además, es bastante común que todas las empresas tengan algunas costumbres que se van pasando de empleado a empleado, y muchas veces no están alineadas con las mejores prácticas o recomendaciones de seguridad más difundidas. Supongamos por un momento que el área de seguridad de una empresa realiza un Vulnerability Assessment o un Penetration Test a la organización (**Figura 8**). No se podría saber hasta qué punto los resultados obtenidos son 100% objetivos y no están marcados por las malas costumbres o por el hecho de saber que si los resultados no son los esperados, la responsabilidad de éstos es propia.

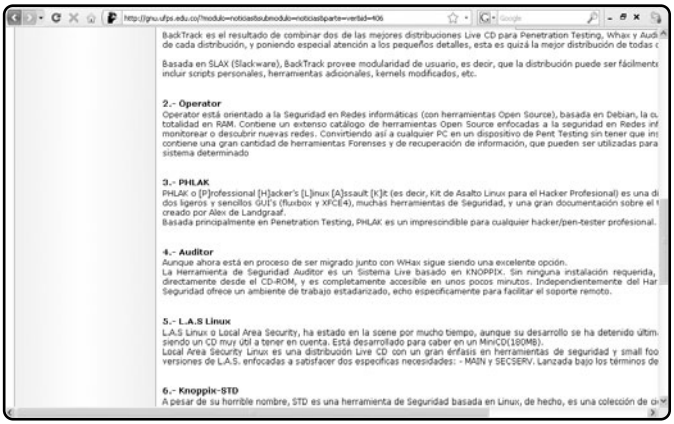


FIGURA 8.
En el sitio web de la Universidad de Francisco de Paula Santander, encontraremos 10 distribuciones de Linux especiales para realizar penetration test.

RESUMEN

En este capítulo, comenzamos viendo los fundamentos necesarios para comprender qué es un Ethical Hacker e introducimos el concepto de los códigos de ética. Luego, analizamos los distintos tipos de ataques y sus características principales.

Multiple **choice**

1 ¿En qué década del siglo XX se empezó a utilizar el protocolo TCP/IP?

a- Cincuenta.
b- Sesenta.
c- Setenta.
d- Ochenta.

2 ¿Cuál de las siguientes capas no pertenece al modelo OSI?

a- Capa de presentación.
b- Capa de sesión.
c- Capa física.
d- Capa de acceso a la red.

3 ¿En qué se basó el modelo de referencia OSI?

a- Protocolo TCP/IP
b- Arpanet
c- DoD
d- ISSA

4 ¿Cómo se llama el estándar internacional de seguridad de la información abierto que promociona y publica contenido de seguridad y normaliza su transferencia por el espectro de herramientas y servicios de seguridad?

a- OVAL
b- CompTIA
c- EC-Council
d- ISC2

5 ¿En dónde se utilizan técnicas de ingeniería social a empleados?

a- Autotesteo y contratación.
b- Evaluación de vulnerabilidades.
c- Penetration test.
d- Ninguna de las anteriores.

6 ¿En cuál de las siguientes se incluye una fase de escaneo?

a- Autotesteo y contratación.
b- Evaluación de vulnerabilidades.
c- Penetration test.
d- Ninguna de las anteriores.

Respuestas: 1-c, 2-d, 3-a, 4-a, 5-c, 6-c.

Capítulo 4

Seguridad física y biometría

Veremos los conceptos relacionados con los procedimientos de control para protección de las amenazas físicas.

Seguridad física y biometría

En este capítulo, veremos los conceptos relacionados con los procedimientos de control para protección de las amenazas físicas, como la biometría y las medidas de protección de accesos, así como también el monitoreo físico dentro y fuera del centro de cómputos.

Conceptos de biometría

La biometría es el estudio de métodos automáticos para el **reconocimiento de personas** basado en rasgos de conducta o físicos. Etimológicamente, proviene del griego **bios** (vida) y **metron** (medida). En nuestro campo, es la aplicación de métodos matemáticos y tecnológicos para identificar o verificar identidad.

CONTEXTO HISTÓRICO

La práctica de la biometría comenzó en occidente a fines del siglo XIX, aunque se cree que ya era utilizada en China en el siglo XIV, donde los comerciantes estampaban en la palma de los niños impresiones en papel con tinta para distinguirlos. En 1883, Alphonse Bertillon, jefe del departamento fotográfico de la Policía de París, desarrolló un **sistema antropométrico** para identificar criminales, que funcionaba mediante la medición de ciertas longitudes y anchos de la cabeza y del cuerpo, y con el registro de marcas características (tatuajes, cicatrices, etcétera). Más adelante, se comenzó a utilizar la huella dactilar para esto mismo (**Figura 1**).

MEDIDAS DE ACEPTACIÓN

Al presentar las características físicas a un sistema, éstas son procesadas y comparadas contra **patrones**. Dado que las mediciones no pueden ser totalmente precisas, el patrón no coincide exactamente, por lo que el sistema se ajusta para ser **flexible**: no tanto como para aceptar un usuario no válido ni tan poco como para que no se lo acepte siendo válido.

VENTAJAS Y DESVENTAJAS

La principal ventaja de un sistema biométrico es su dificultad para falsificarlo. Además, no puede ser transferido, no puede olvidarse y no requiere esfuerzo para su uso. Respecto de sus desventajas, la principal es su costo elevado.

La práctica de la biometría comenzó en occidente a fines del siglo XIX

Las medidas de aceptación se definen en función de la **tasa de falsa aceptación** (*False Acceptance Rate* o **FAR**) y la **tasa de falso rechazo** (*False Rejection Rate* o **FRR**). Por como están concebidos, al aumentar uno disminuye el otro, por lo que se define otra medida para la que ambas son iguales, llamada **tasa de error igual** (*Equal Error Rate* o **EER**), o **tasa de error de cruce** (*Cross-over Error Rate* o **CER**, ver **Figura 2**). Otros factores asociados son el **enrollment time** (tiempo de evaluación), el **throughput rate** (tasa de procesamiento), la aceptabilidad (consideraciones de privacidad, psicológicas, etcétera) y la precisión intrínseca.

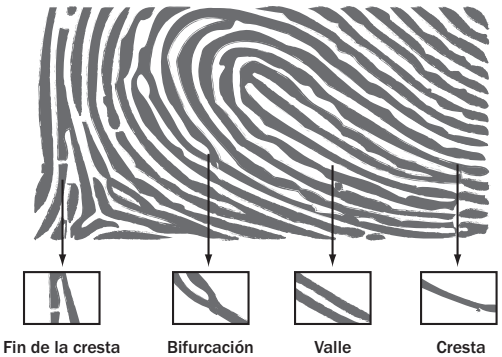


FIGURA 2. La CER se mide en el cruce entre la FAR y la FRR, y se considera que el sistema es más exacto cuanto más bajo es este índice.

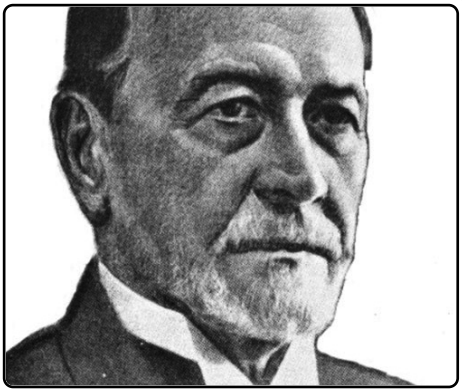


FIGURA 1. Juan Vucetich desarrolló y puso en práctica por primera vez un sistema de identificación de personas por huellas digitales.

ESTÁNDARES EXISTENTES

El principal organismo internacional de estandarización biométrica es el subcomité 17 del grupo JTC1 de ISO/IEC. Estados Unidos, por su parte, cuenta con otras organizaciones como ANSI (**www.ansi.org**) y NIST (**www.nist.gov**). También hay organismos no gubernamentales como Biometrics Consortium (**www.biometrics.org**), International Biometrics Groups (**www.biometricgroup.com**) y BioAPI Consortium (**www.bioapi.org**). Los estándares más importantes son:

- **ANSI/INCITS 358** o **BioAPI**: creado en 2001, presenta una interfaz de programación que garantiza **interoperabilidad**.
- **NISTIR 6529** o **CBEFF** (*Common Biometric Exchange File Format*): creado en el año 1999 por el NIST y Biometrics Consortium, nos propone una estructura de datos para el intercambio de información biométrica.

- **ANSI X.9.84**: creado en 2001, define las condiciones de los sistemas para la industria financiera, y se refiere a cuestiones como la transmisión, el almacenamiento y el hardware.

Elementos fisiológicos y psicológicos

Los elementos utilizados en biometría pueden ser **estáticos**, como las huellas dactilares, la retina, el iris, los patrones faciales, las venas de la mano y la geometría de la palma, o bien **dinámicos** (de comportamiento), como la firma y el tecleo. La voz, por su parte, se considera una mezcla de características físicas y de comportamiento.

ACERCA DE LAS HUELLAS DACTILARES

Una huella dactilar aparece como una serie de líneas oscuras (relieves) y espacios en blanco (bajorrelieves). La medición automatizada requiere gran poder de procesamiento y almacenamiento, por lo que estos sistemas se basan en **rasgos parciales**.

Una huella dactilar aparece como una serie de líneas oscuras (relieves) y espacios en blanco (bajorrelieves)

Para captar la huella se utilizan **sensores** como los **ópticos**, que toman una imagen común de la huella. Éstos son los más usados. También hay **capacitivos**, que determinan el calor de cada punto basados en la capacidad eléctrica. Otros utilizan **ultrasonido** o **prismas** para detectar cambios en la reflectancia de la luz (**Figura 3**).

En cuanto a la determinación de coincidencias, puede basarse en **minucias** (medición de la ubicación de los puntos característicos) o en **patrones** (comparación simple de imágenes).

RECONOCIMIENTO FACIAL

Entre las tecnologías biométricas, ésta es una de las más nuevas y es muy aceptada porque es una forma común de reconocerse entre personas (**Figura 4**). Hay dos enfoques predominantes: el **geométrico** (basado en rasgos) y el **fotométrico** (basado en lo visual).

LA ÚNICA HUELLA

En 1686, Marcello Malpighi señaló las diferencias entre **crestas**, **espirales** y **lazos** en las huellas dactilares. Hoy sabemos que las huellas son la característica humana más singular después del ADN, y la probabilidad de que se repitan entre dos personas es 1/64.000 millones.

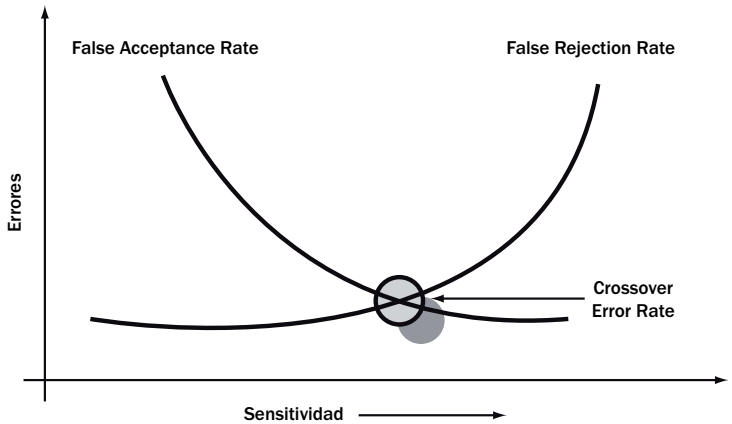


FIGURA 3. Un sistema automatizado de identificación de huellas dactilares, o AFIS ***(Automated Fingerprint Identification System)*****, interpreta el flujo de las crestas sobresalientes para clasificar las huellas y extraer los detalles de un conjunto de las minucias.**

Los tres algoritmos más estudiados fueron: análisis de componentes principales (*Principal Components Analysis*, **PCA**), análisis lineal discriminante (*Linear Discriminant Analysis*, **LDA**) y correspondencia entre agrupaciones de grafos elásticos (*Elastic Bunch Graph Matching*, **EBGM**).

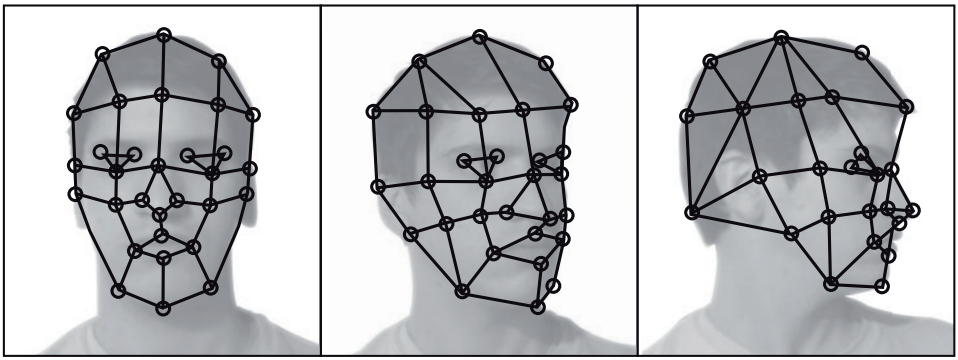


FIGURA 4. Correspondencia entre agrupaciones de grafos elásticos**. La dificultad del método es la localización del punto de referencia, que puede ser obtenido al combinar** PCA **y** LDA**.**

EL IRIS Y LA RETINA

El iris es una membrana de color ubicada en el ojo, más precisamente entre la córnea y el cristalino, y su función es regular la cantidad de luz que llega, variando el tamaño de la pupila. Para su reconocimiento, primero se realiza la localización y luego la extracción de características (**Figura 5**), que se comparará con patrones previa aplicación de procesos matemáticos (es una de las tecnologías más exactas).

La ubicación y la disposición de los vasos sanguíneos de la retina es única para cada ser humano (dato comprobado en 1935), por lo que el patrón se utiliza como medio de identificación. Para esto, el usuario debe acercar el ojo al lector y fijar su mirada en un punto, para que se examinen sus patrones (a diferencia del iris, no se puede usar lentes). Una gran ventaja de este método es que el órgano cadavérico no tiene utilidad para el reconocimiento.

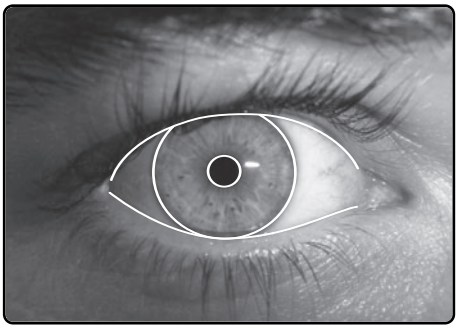


FIGURA 5. En el reconocimiento de iris, los contornos blancos indican la localización de los límites de éste y del párpado.

LA VOZ HUMANA

El reconocimiento por el habla es considerado uno de los más naturales, ya que también es utilizado por el ser humano para identificar a otros. Su estudio data de mediados de los años 60, cuando se estableció que los patrones y las frecuencias con los que cada persona dice una palabra son únicos.

El reconocimiento de voz funciona mediante la digitalización del habla (**Figura 6**). Cada palabra se descompone en **segmentos** que tienen tonos dominantes, y se plasman en un espectro para

HISTORIA, IRIS Y PATENTES

En 1936, el oftalmólogo Frank Burch propuso usar patrones de iris, pero recién en 1985 Leonard Flom y Aran Safir retomaron la idea. Para 1994, los algoritmos patentados por Daugman fueron la base para los productos de reconocimiento del iris.

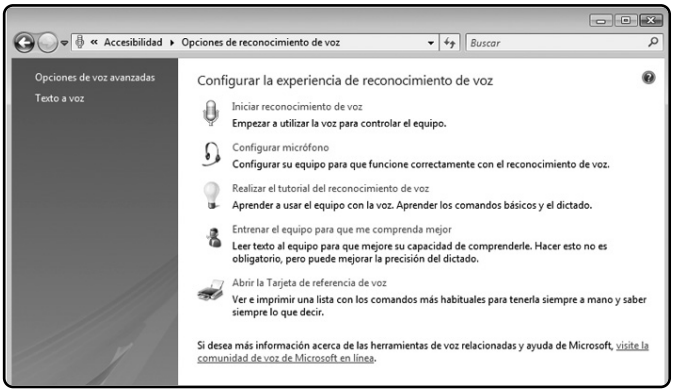


FIGURA 6.
Windows Vista incluye la característica de reconocimiento de voz, lo que permite ejecutar comandos y aplicaciones del sistema mediante el dictado de órdenes.

conformar el **voice print** (plantilla de la voz). El sistema es muy susceptible a cambios causados por disfonía, fatiga y otras afecciones. Cabe destacar que el reconocimiento de palabras no es lo mismo que el reconocimiento de la voz, aunque pueden combinarse para obtener un sistema más preciso.

LA FIRMA

El reconocimiento por firma es poco problemático y bien aceptado, dado que estamos muy habituados a usarla como método de reconocimiento. El proceso de análisis se realiza en dos áreas: la firma en sí y el modo en el que se lleva a cabo. Los datos tomados son la velocidad, la presión, la dirección, el largo del trazo y las áreas donde se levanta el lápiz (**Figura 7**). El inconveniente principal es que nunca se firma dos veces igual, por lo que deben ajustarse los patrones.

FIGURA 7. El reconocimiento de firma es muy aceptado y se utiliza principalmente en bancos e instituciones financieras.

PRIVACIDAD Y BIOMETRÍA

La biometría puede disminuir la privacidad de los ciudadanos, al dar a conocer los detalles sobre las personas y su correlación con otros datos de su perfil. Por ejemplo, es posible conocer, a partir del número de documento de alguien, su huella digital o su rostro.

Amenazas a la seguridad física

Las amenazas son hechos que pueden producir daño y causar pérdidas de activos. Existe la posibilidad de que ocurran en cualquier momento. Se pueden dividir en:

- **Naturales**: condiciones de la naturaleza y la intemperie (fuego, inundación, terremoto, etcétera). Normalmente, se recurre al pronóstico del clima para conocer estos avisos, ya que la probabilidad está estudiada.
- **Humanas**: relacionadas con daños cometidos por las personas. Pueden ser intencionales (con intención de daño deliberado, como vandalismo, fraudes, sabotajes, espionaje, etcétera) o no intencionales (resultantes de acciones inconscientes).

Protección del datacenter

La **seguridad física** consiste en la aplicación de barreras físicas y procedimientos de control para protección de las amenazas a los recursos, tanto del **datacenter** (**DC**) o **CPD** (Centro de Procesamiento de Datos), como del resto de la empresa. Por la información que contiene, ésta es, sin dudas, la habitación más protegida de un entorno corporativo. Su estructura interior es bastante particular en comparación con otros ambientes. En el ingreso, suelen utilizarse procedimientos donde quede constancia del acceso y de las acciones que realiza cada persona que entra, para un futuro análisis.

UBICACIÓN INTERNA

La ubicación del DC dentro de las instalaciones de la empresa determina, en parte, su seguridad. Existen muchos criterios de definición, pero la mayoría coincide en algunos puntos, por ejemplo, que no se debe ubicar en subsuelos ni en el último piso de la edificación. De forma ideal, se pretende un piso entero dedicado y, cuanto más discreta sea la ubicación,

DEFENSA EN CAPAS FÍSICAS

La defensa en capas utilizada en aspectos tecnológicos también se aplica en seguridad física. Así, pueden definirse estratos que van desde el perímetro externo, pasando por las entradas, las oficinas y los pasillos internos hasta llegar al datacenter.

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control para protección de las amenazas a los recursos

mejor será a los fines de la seguridad y disuasión. También debe tenerse en cuenta su ubicación con respecto a los demás sectores, oficinas y sitios de alto tránsito de personas. Otra recomendación es que no esté próximo a instalaciones industriales y fuentes de radiación electromagnética.

CATEGORÍAS TIER

El standard **TIA-942** (*Telecomunication Infrastructure Standard for Data Centers*) incluye un anexo informativo sobre los grados de disponibilidad con los que pueden clasificarse los DC, basados en información del **Uptime Institute** (**www.uptimeinstitute.org**):

- **Tier I - DC básico**: puede admitir interrupciones planeadas y no planeadas. La carga máxima en situaciones críticas es del 100% y la tasa de disponibilidad máxima es del 99.671% del tiempo.
- **Tier II - Componentes redundantes**: menos susceptible a interrupciones y conectado a una sola línea de electricidad. Existe, al menos, un duplicado de cada componente y la carga máxima en situaciones críticas es del 100%. La disponibilidad máxima es del 99.741%.
- **Tier III - Mantenimiento concurrente**: admite actividades planeadas sin interrupciones de operación y posee doble línea de electricidad. La carga máxima en situaciones críticas es del 90% y la disponibilidad máxima es del 99.982%.
- **Tier IV - Tolerante a fallas**: capacidad para realizar cualquier actividad planeada sin interrupcio nes de servicio y con tolerancia a fallas. Requiere dos líneas de distribución activas simultáneas. La carga máxima en situaciones críticas es del 90% y la disponibilidad máxima es del 99.995%.

SISTEMAS DE ALIMENTACIÓN ELÉCTRICA

La energía eléctrica es indispensable para el funcionamiento de los sistemas, pero las compañías de servicios no pueden asegurar suficiente disponibilidad como se esperaría.

Esta situación se traduce en la necesidad de contar con sistemas alternativos de provisión, como **grupos electrógenos** o **generadores** (**Figura 8**).

DATACENTER TIPO BÚNKER

A la hora de construir un datacenter, se habla de búnker para hacer referencia a una sala construida en concreto de alta resistencia en paredes, techo y piso, con una estructura exterior que impide impactos directos comunes.

FIGURA 8. Los generadores eléctricos funcionan con combustible diesel o similar.

Los dispositivos complementarios son los sistemas de **alimentación ininterrumpida** o **UPS** (*Uninterruptible Power Supply*), que pueden proteger contra cortes, bajas de tensión, variación de frecuencia, ruido de línea, picos de tensión, caídas y transitorios de electricidad. La unidad para determinar la capacidad de una **UPS** es el Volt Amper (**VA**). Una **UPS** almacena energía en baterías especiales para interiores y se usa para proveer electricidad por tiempos no muy prolongados.

VENTILACIÓN Y AIRE ACONDICIONADO

El **acondicionamiento de aire** consiste en regular las condiciones de temperatura (calefacción o refrigeración), humedad, limpieza (renovación y filtrado) y movimiento del aire en los ambientes (**Figura 9**). Si solo hacemos referencia a la temperatura, hablamos de **climatización**. Los sistemas de acondicionamiento se suelen llamar **HVAC** (*Heating, Ventilating and Air Conditioning*, o Calefacción, Ventilación y Aire acondicionado).

El acondicionamiento de aire consiste en regular las condiciones de temperatura (calefacción o refrigeración)

En un DC, a fin de evitar el calentamiento de servidores, la **temperatura** debe estar entre los 22°C y los 24°C, y la humedad entre el 45% y el 55%.

En cuanto a la ventilación, en DCs utilizamos **ventilación forzada**, que se realiza mediante conductos de distribución y funciona mediante extractores y ventiladores. Este tipo de ventilación proporciona movimiento al aire para que circule de la manera prevista entre los racks de servidores y pasillos.

TODO REQUIERE ELECTRICIDAD

Los sistemas de alarmas y controles de acceso perimetrales dependen también de la energía eléctrica, por lo que deben ser considerados a la hora de planificar, ya que no es deseable que, por falta de electricidad, dejen de funcionar y generen una brecha.

FIGURA 9. Los sistemas de acondicionamiento de aire para interiores deben ser calculados en función del volumen de la habitación, en metros cúbicos.

FIGURA 10. El piso técnico permite pasar cables de electricidad y datos por debajo de él.

PISOS, TECHOS Y PAREDES

En un DC, hay que utilizar el denominado **piso técnico**, conformado por **placas** intercambiables fabricadas a partir de planchas de acero, en general, pintadas con pintura **epoxi** (**Figura 10**). Las placas brindan rigidez estructural y aislación acústica, además de ser **ignífugas**.

También existen los **techos técnicos**, concebidos por placas sujetas por perfiles longitudinales de aluminio de gran sección y resistencia. Estos techos falsos son **registrables**, lo que significa que es posible acceder a lo que hay sobre ellos sin romperlos.

Finalmente, las **paredes** deben ser de materiales ignífugos con tolerancia de, al menos, una hora y lo suficientemente resistentes como para minimizar la posibilidad de penetraciones. Además, deben incluir aislación sonora, contra el agua y la humedad.

DETECCIÓN Y SUPRESIÓN DE INCENDIOS

Un incendio implica la ocurrencia no controlada de fuego que afecta las estructuras y a los seres vivos, incluso, puede producir la muerte por inhalación de humo y quemaduras. Para que se inicie el fuego son necesarios tres factores: **combustible**, **comburente**

SEGURIDAD FÍSICA ILUMINADA

La iluminación es un factor importante a considerar en la seguridad física, ya que se estudian de forma especial las áreas que se van a iluminar y el tipo de luz que va a ser utilizado en cada lugar, en función del tipo de uso que tenga y del tiempo que deba permanecer encendida.

(oxígeno) y **calor**. La eliminación de cualquiera de éstos provoca la extinción del fuego (**Figura 11**). Las normativas clasifican el riesgo para poder adecuar los medios de prevención. En Estados Unidos, se distingue entre las siguientes clases de fuego:

FIGURA 11. Las prevenciones contra la acción del fuego buscan salvar vidas y minimizar pérdidas. El matafuegos es la medida más básica de seguridad.

- Clase A: combustibles comunes sólidos (madera, papel, telas, gomas, entre otros).
- Clase B: combustibles líquidos (aceites, nafta, grasas, ceras, pinturas, etcétera).
- Clase C: fuego eléctrico sobre materiales e instalaciones o equipos (cortocircuito, fallas en cables).
- Clase D: combustibles metálicos (magnesio, titanio, potasio, sodio, mercurio, etcétera).

Las medidas pueden ser **pasivas**, cuando se refieren a la constitución del entorno para evitar la propagación del fuego, o bien **activas**, que implican los mecanismos de extinción que van a ser accionados. A su vez, las activas pueden ser de **detección** (de humo, llama o calor), de **alerta** y **señalización** (sonora o luminosa) y de **extinción** (matafuegos, rociadores, etcétera). Ver **Figura 12**.

Acceso a las instalaciones

El control en los accesos a las instalaciones de una empresa determina la **protección de los activos**; debe tenerse en cuenta desde el perímetro externo hasta las vías de ingreso a los edificios, las oficinas y el DC.

FABRICANTES ELITE

Algunos fabricantes internacionales destacados de dispositivos y sistemas de control perimetral son Magal Security Systems (Israel, **www.magal-ssl.com**), Senstar Stellar (Canadá, **www.senstarstellar.com**) y Delta Scientific (EE.UU., **www.deltascientific.com**).

FIGURA 12. Un rociador (sprinkler) es un dispositivo para extinción de incendios, que libera una lluvia de agua sobre la zona afectada.

SEGURIDAD PERIMETRAL

La seguridad perimetral se refiere a un conjunto de elementos integrados (informáticos, electrónicos y mecánicos) destinados a la protección de perímetros y detección de intrusos físicos. Según la cobertura, pueden clasificarse como **volumétricos**, **superficiales** y **lineales**, aunque también pueden dividirse por su principio físico de actuación (**Figura 13**).

Si bien su mayor área de desarrollo y aplicación es la seguridad nacional en instalaciones militares, gubernamentales, prisiones, fronteras, aeropuertos y demás, también se destaca su uso en industrias, sedes de empresas, residencias de alto nivel, etcétera.

PUERTAS Y VENTANAS

Las puertas son las vías de acceso tradicional a un ambiente, pero deben tenerse en cuenta las ventanas como vía alternativa para un atacante (**Figura 14**). En el caso de un DC, éste no tendrá que poseer ventanas, y en el resto de las oficinas hay que conocer los requerimientos para ellas (insonorización, aislamiento térmico, etcétera).

En cuanto a las puertas, se deberán utilizar las de alta seguridad para prevenir impactos e ingresos por

FIGURA 13. Las medidas de seguridad perimetral pueden incluir una torre de vigilancia y alambrado para evitar accesos no autorizados desde el entorno.

FIGURA 14. Las puertas pueden incluir cerraduras activadas por tarjeta magnética para aumentar la seguridad en el acceso.

la fuerza, y las cerraduras deberán ser adecuadas para ofrecer medidas de control de los ingresos, ya que de nada sirve que la entrada esté asegurada si cualquiera puede acceder. Las puertas de alta seguridad pueden incluir barras de acero reforzado en su interior, por lo que también son más pesadas (**Figura 15**).

FIGURA 15. Las bóvedas de seguridad de bancos poseen puertas de acceso con el mayor nivel de seguridad disponible en el mundo.

ABRIR CERROJOS: LOCKPICKING

Se conoce como **lockpicking** (del inglés **lock**, que significa cerradura, y **pick**, ganzúa) a la apertura de cerraduras por medio de técnicas y herramientas especiales que no incluyen la llave original. La teoría del lockpicking habla de explotar los defectos mecánicos, lo cual requiere conocer teoría acerca del funcionamiento de los distintos sistemas (**Figura 16**).

LA BIBLIA DEL LOCKPICKING

Un texto revolucionario sobre lockpicking fue **The MIT Guide to Lock Picking** (1991), referido a la apertura de cerraduras y candados con métodos alternativos. En 1992, se cambió el título de la publicación por quejas del **MIT** sobre la inclusión del nombre institucional.

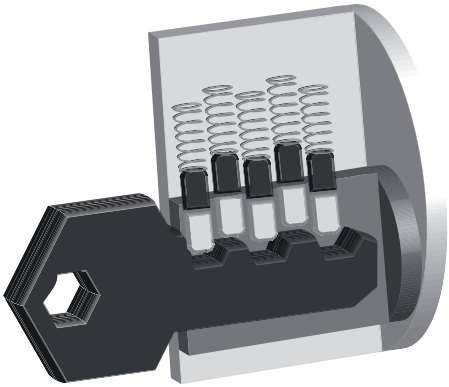


FIGURA 16. Se debe empujar hasta sentir que se ha colocado en la línea de corte y repetir hasta vencer todos los pernos.

Los sistemas más modernos requieren técnicas refinadas y más paciencia, incluyendo el manejo de la presión de las ganzúas, el ajuste de tensión, y la identificación táctil de los mecanismos internos. El factor más apreciado es el tiempo que se demora en abrir una cerradura y no la apertura en sí, y es a lo que apuntan los mecanismos modernos (**Figura 17**).

CERRADURAS ELECTRÓNICAS

Una cerradura electrónica es un dispositivo que opera igual que una cerradura, pero con la ayuda de un

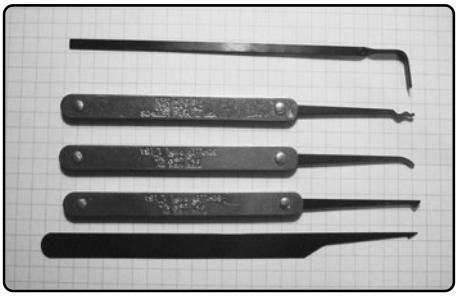


FIGURA 17. Los juegos de ganzúas son una herramienta indispensable para el lockpicking.

circuito eléctrico. Muchas veces funcionan con un panel montado sobre ellas y otras veces se interconectan con un sistema de control de accesos centralizado para realizar validaciones, permitir el registro de intentos de apertura y el bloqueo del acceso. La **autenticación** puede ser realizada por medio de códigos numéricos, **tokens** o mecanismos biométricos, y son una buena alternativa a las tradicionales por su flexibilidad, aunque son bastante más costosas por su mayor mantenimiento (**Figura 18**).

Los sistemas más modernos requieren técnicas refinadas

DÓNDE ESTÁ LA CLAVE

Entre los métodos de obtención de claves para cerraduras electrónicas, los más frecuentes son el de espiar al sujeto que la introduce (**shouldersurfing**) y el de analizar con luz infrarroja el teclado para detectar las teclas que tienen mayor cantidad de huellas digitales.

FIGURA 18. Las cerraduras electrónicas cuentan con su propio sistema de alimentación

Quién **está allí**

Uno de los objetivos de la seguridad física es la **detección** de personas no autorizadas en los entornos que se desea **monitorear**. Para esto, se utilizan distintos métodos orientados a brindar información sobre lo que está ocurriendo.

SISTEMAS DE ALARMA

Los sistemas de alarma alertan sobre acciones potencialmente peligrosas en un ambiente determinado y, al ser elementos **pasivos**, no evitan intrusiones (**Figura 19**). Se piensan como **pólizas de seguro** porque es necesario tenerlas, pero se espera necesitarlas.

Los dispositivos pueden estar conectados con una **central de monitoreo** que recibe las señales de los sensores a través de algún medio (línea telefónica, GSM, radiofrecuencia, etcétera) o cumplir la función disuasoria con la activación de una **sirena** de alrededor de 90 decibeles. En general, se alimentan por corriente alterna y una batería de respaldo.

DETECCIÓN DE MOVIMIENTO Y MÁS

Los **detectores** pueden emplear diferentes tecnologías según lo que se desea detectar y considerar como peligroso. Por ejemplo, pueden sensar cambios de **temperatura** y **movimiento** (pensados para la detección de personas), apertura de puertas y ventanas mediante elementos magnéticos, cambios volumétricos en un recinto, sonidos ambientales, etcétera. También hay sensores inerciales para detección de golpes, que son usados en cajas fuertes, puertas, paredes y ventanas. Los detectores de rotura de

LOS CAZADORES DE MITOS

Durante 2007, en un programa de televisión de Discovery Channel llamado **Cazadores de Mitos** (**Mythbusters**), se realizaron pruebas sobre la detección de cada sistema de alarma moderno y se demostró que era posible violar sus medidas de seguridad.

FIGURA 19. Muchos sistemas de alarma cuentan con un teclado numérico que permite activarlo y desactivarlo.

cristales, por ejemplo, sensan la frecuencia de sonido de una rotura de cristal. Cada sistema tiene asociadas técnicas de evasión, bien conocidas por los atacantes (**Figura 20**).

FIGURA 20.
Los sensores de movimiento disparan el encendido de una luz si detectan la presencia de una persona.

MONITOREO Y VIGILANCIA

Los sistemas de monitoreo permiten la **visualización**, con o sin grabación, de todo lo que sucede en un recinto, según lo captado por cámaras estratégicamente ubicadas. Las cámaras pueden estar a la vista (para actuar como medida disuasiva) u ocultas (para evitar que el intruso sepa que está siendo captado), pero los monitores del sistema estarán ubicados en un sector de alta seguridad. Los elementos del sistema poseen protección contra sabotaje, de manera que si se corta la alimentación o se produce la rotura de alguno de sus componentes, se enviará una señal a la central de alarma.

PERSONAL DE SEGURIDAD

Los servicios de personal de vigilancia están encargados del control de acceso a un edificio donde circula gran cantidad de gente, o bien de la periferia y zonas restringidas. Los guardias de seguridad son quienes cumplen con esa tarea y, por lo general, visten ropas fácilmente reconocibles para poder ser identificados.

RESUMEN

En este capítulo, describimos la biometría y enumeramos algunos de los elementos principales del cuerpo humano que son estudiados. También presentamos la seguridad a nivel del datacenter y las amenazas fundamentales que de ésta se desprenden.

Multiple **choice**

1 ¿En qué siglo comenzó la práctica de la biometría en occidente?

a- XVIII
b- XIX
c- XX
d- XXI

2 ¿Cuál de las siguientes no representa una amenaza natural?

a- Fuego.
b- Inundación.
c- Espionaje.
d- Terremoto.

3 ¿Dentro de qué medidas activas se encuentran los rociadores?

a- Detección.
b- Alerta.
c- Señalización.
d- Extinción.

4 ¿Qué clase de riesgo son los cortocircuitos?

a- Clase A.
b- Clase B.
c- Clase C.
d- Clase D.

5 ¿Qué clase de riesgo lleva la combustión de la madera?

a- Clase A.
b- Clase B.
c- Clase C.
d- Clase D.

6 ¿Cuál de las siguientes opciones no es una clasificación de la seguridad perimetral?

a- Volumétricos.
b- Superficiales.
c- Lineales.
d- Cuadrangulares.

Respuestas: 1-b, 2-c, 3-d, 4-c, 5-a, 6-d.

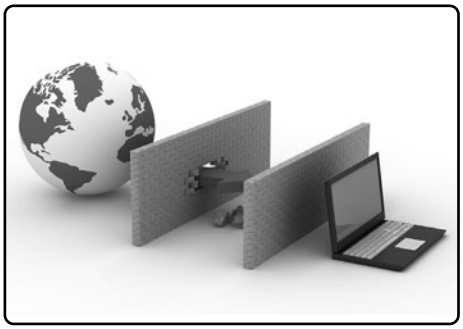
Capítulo 5

Amenazas en entornos web

En este capítulo, analizaremos los componentes, las tecnologías y los protocolos relacionados con la Web.

Amenazas en entornos web

En este capítulo, nos dedicaremos enteramente al mundo web y a sus problemas asociados. El especial foco que hacemos sobre esto tiene su razón en el hecho de que la Web funciona como base para muchas cosas, y es por esto también que los hackers le prestan tanta atención. En definitiva, el mundo del puerto 80 requiere un especial cuidado.



El mundo web

Lo que conocemos como **WWW** (*World Wide Web*) nació como un proyecto de índole militar, al igual que muchos otros avances de la ciencia y la tecnología. Esta estructura de comunicaciones permitió interconectar puntos remotos por medio de un **protocolo** predefinido (**TCP/IP**). Con esta nueva arquitectura se desarrollaron los modelos de comunicaciones y se definieron jerarquías (clientes y servidores) que dieron origen a una revolución digital.

Los protocolos y la red cumplían con los requerimientos funcionales, pero no habían sido concebidos para ser estrictamente seguros, por lo que no pasó mucho tiempo hasta que algunos intentaron hacer abuso de ellos con distintos métodos de ataques. Esto obligó a estudiar los diferentes modos de ataque y sus contramedidas, basados principalmente en el uso apropiado de las mismas tecnologías y lenguajes existentes.

EL PROTOCOLO HTTP

Cuando hablamos de la Web, lo primero que viene a la mente es el **protocolo HTTP** (*HyperText Transfer Protocol*), que permite el intercambio de información a través de Internet (**Figura 1**). Trabaja en el **puerto TCP 80** y, conceptualmente, es muy simple.

Las conversaciones entre los extremos (cliente y servidor) se llevan a cabo por medio de instrucciones

CGI Y LOS SERVIDORES WEB

Los primeros servidores web permitían visualizar solo información estática. Una solución a eso consistía en ejecutar programas que se encontraran dentro del servidor. Esta tecnología se conoció como **CGI** (*Common Gateway Interface*).

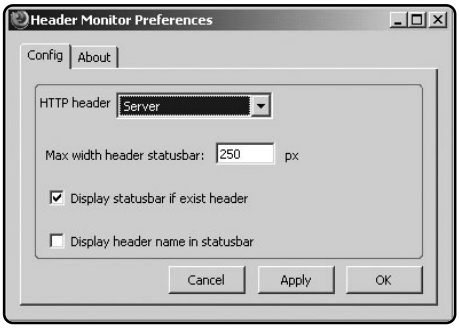


FIGURA 1. Header Monitor es un plugin para Firefox, que muestra el estado de respuestas HTTP en la barra de estado del navegador (Server, Content-Encoding y Content-Type).

llamadas **métodos**. A partir de éstos es posible establecer solicitudes o **requerimientos**, que serán respondidos con **mensajes**. Para conocer más, se puede recurrir a los **RFCs** (**Figura 2**).

En la **Tabla 1**, podemos ver una lista de los métodos más utilizados en HTTP junto con un ejemplo de **petición** (requerimiento o *request*) que conforma la **URI** (*Uniform Resource Identifier*) y la explicación de su uso. La URI es un identificador de recursos que se encuentra definido en la **RFC 2396** y se compone de una cadena de caracteres que los identifica unívocamente.

CODIFICACIÓN DE CARACTERES

La técnica de *encoding*, o codificación de caracteres, utilizada en documentos HTML, permite convertir un carácter de un lenguaje natural en un símbolo de otro sistema de representación mediante la aplicación de reglas. Uno de los más importantes es el **ASCII** (*American Standard Code for Information Interchange*), de 8 bits (7 más uno de paridad), que solo puede codificar **128 símbolos**.

FIGURA 2. El sitio www.rfc-es.org tiene como objetivo ofrecer las traducciones de los RFC estándar originales del inglés al español.

MÉTODO	REQUERIMIENTO	USO
GET	GET <Request-URI>?query_ string HTTP/1.1\r\n Host: <hostname o IP>\r\n\r\	Recuperar información identificada por un URI. Se utiliza para pasar información al servidor en forma de valores al final del URI tras un signo de interrogación.
POST	POST <Request-URI> HTTP/1.1\r\n Host: <hostname o IP>\r\n Content-Length: <longitude_bytes> \r\n Content-Type: <content type> \r\n\r\n <query_string Request-URI>	Invocación de páginas como respuesta a peticiones. Además, aporta datos de entrada (pares atributo/valor).
HEAD	HEAD <Request-URI> HTTP/1.1\r\n Host: <hostname o IP>\r\n\r\n	Es similar a GET, pero no se devuelve el cuerpo en la respuesta. Obtiene datos sobre el servidor sin transferir la página.
PUT	PUT <Request-URI> HTTP/1.1\r\n Host: <hostname IP>\r\n Content-Length: <length in bytes>\r\n Content-Type: <content type>\r\n\r\n <data to put to file>	Guardar el contenido de la petición en el servidor tras la URI requerida.
OPTIONS	OPTIONS <Request-URI> HTTP/1.1\r\n Host: < hostname o IP>\r\n\r\n	Petición sobre las opciones de comunicación disponibles.
DELETE	DELETE <Request-URI> HTTP/1.1\r\n Host: < hostname o IP>\r\n\r\n	Eliminar del servidor el recurso indicado por la URI solicitada.
TRACE	TRACE <Request-URI> HTTP/1.1\r\n Host: < hostname o IP>\r\n\r\n	Conocer si existe un receptor y obtener información de diagnóstico.
CONNECT	CONNECT <Request-URI> HTTP/1.1\r\n Host: < hostname o IP>\r\n\r\n	Especificar la información de un proxy al recurso identificado por la URI.

TABLA 1. Métodos y definiciones del protocolo HTTP 1.1.

Un documento HTML debería contener una declaración del set de caracteres (charset) en su encabezado

Si bien 7 bits son suficientes para incluir mayúsculas y minúsculas del abecedario inglés, cifras, puntuación y caracteres de control, no se incluyen caracteres acentuados y otros símbolos.

Así, nace **ASCII Extendido**, con varios códigos de 8 bits, definidos para lenguas con escritura semejante, aunque tampoco dan una solución unificada. Con esto en mente, surge el estándar **Unicode** (*Unicode Industrial Standard*), que tiene por objetivo unificar las codificaciones, con esquemas **UTF** (*Unicode Transformation Format*), (**Figura 3**). Existen varios sets, como el UTF-8, de 8-bits de longitud variable y compatible con ASCII, que usa entre 1 y 4 bytes para la codificación de un carácter (8 a 32 bits), según el símbolo (también existe UTF-16, de 16 bits).

Un documento HTML debería contener una declaración del set de caracteres (**charset**) en su encabezado. Los símbolos se pueden insertar con un código que se asocia a un carácter específico, decimal o hexadecimal. La escritura de símbolos depende del tipo de fuente del navegador y muchos no dan soporte para todos los caracteres estándar. Los caracteres no soportados son mostrados como cuadrados o signos de interrogación.

AUTENTICACIÓN WEB

Los servidores y aplicaciones web permiten varios mecanismos de autenticación. El más común es el HTTP, que puede dividirse en:

DoS A USUARIOS Y SERVIDORES

En un ataque contra un usuario específico, un intruso intentará validarse con una contraseña errónea para que se bloquee al usuario verdadero. En un ataque contra un servidor web, puede enviarse una petición para aprovecharse de una vulnerabilidad en el sistema.

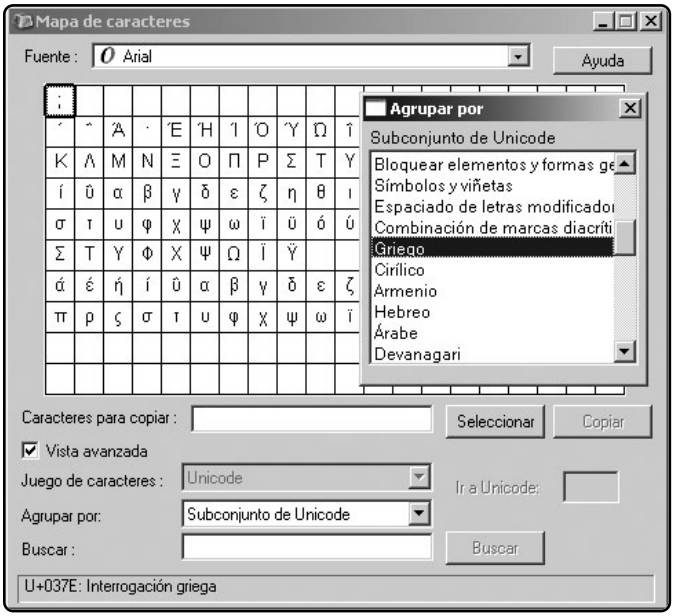


FIGURA 3.
El mapa de caracteres de Windows permite seleccionar un subset de caracteres de un formato específico, en este caso caracteres griegos de Unicode.

- Básica: el cliente envía usuario y contraseña al servidor en texto plano.
- Por **digest**: se calcula el hash de la contraseña y se utiliza un desafío-respuesta para validar sin enviar la contraseña.

Los servidores y aplicaciones web también permiten autenticación basada en **NTLM**, **certificados**, **tokens** y **biometría**. La autenticación NTLM es la mejor opción en un entorno puramente Microsoft, aunque pueden utilizarse sistemas más complejos como Kerberos. Para sistemas PKI se utilizan tecnologías de clave pública y privada con certificados X.509. Para los tokens, se emplean dispositivos de hardware, como segundo factor de autenticación, combinado con otro mecanismo como usuario/password.

¿INYECCIÓN EN ASP?

ASP es la tecnología de desarrollo web de Microsoft. En el caso que exista la inyección de código que se consiga utilizando ASP, estaremos hablando de **ASP Injection**. En la práctica, la técnica también se usa para la explotación de vulnerabilidades de evaluación dinámica.

Beneficios de las **aplicaciones web**

Mucho se ha hablado sobre las ventajas que tiene el hecho de llevar el software a servidores que puedan ser accedidos por medio del protocolo HTTP.

De hecho, éste es uno de los beneficios que caracterizan las aplicaciones web. Para encontrar una definición, podemos recurrir a la guía *OWASP - A Guide to Building Secure Web Applications and Web Services*, que dice: una aplicación web es un software cliente/servidor que interactúa con usuarios y sistemas utilizando HTTP. Desde el punto de vista del usuario, el cliente suele ser un **navegador**, en tanto que para las aplicaciones convencionales sería cualquier **http User Agent**, es decir, una aplicación que manejara ese protocolo.

Algunos ejemplos de aplicaciones web son los webmails, los foros, las redes sociales online y los blogs. La forma de encarar la seguridad en las aplicaciones web es distinta del método empleado en aplicaciones comunes, conformadas por archivos ejecutables y librerías sobre el sistema operativo.

El hecho de que las aplicaciones web estén cada vez más difundidas hace que una buena parte de la seguridad ya esté concentrada en ellas.

Por otro lado, muchas de las técnicas de ataque son sencillas y no hace falta contar con un gran conocimiento técnico para llevarlas a cabo (solo un navegador, pericia en el uso de un buscador, herramientas adecuadas y paciencia). Además, las vulnerabilidades en las aplicaciones web pueden ser explotadas con independencia de la plataforma sobre la cual se están ejecutando.

Los servidores y aplicaciones web permiten varios mecanismos de autenticación

USOS DE LA INYECCIÓN

La inyección de código puede utilizarse para modificar una base de datos, instalar malware usando navegadores como interfaz con el SO, elevar privilegios mediante explotación de código consola, y robar sesiones con HTML y scripts.

El método usado para determinar el riesgo no es tan importante como el hecho de hacerlo de forma estructurada

EL MODELADO DE LAS AMENAZAS

Esta es una técnica para la identificación de las amenazas, ataques, vulnerabilidades y contramedidas que pueden existir en una aplicación. El proceso es llamado **threat modeling** y es necesario para calcular la probabilidad y el impacto de las violaciones de seguridad. Un modelo de amenazas realiza una evaluación y clasificación de las posibles amenazas, y propone técnicas de **defensa**.

El método usado para determinar el riesgo no es tan importante como el hecho de hacerlo de forma estructurada, y de allí la necesidad de adoptar algún modelo. Uno de los más conocidos es el de Microsoft, que propone: identificar los objetivos de seguridad, armar una descripción general de la aplicación, separar los componentes, identificar las amenazas, e identificar y documentar las vulnerabilidades.

El modelo incluye los esquemas llamados STRIDE y DREAD. **STRIDE** es una representación de las posibles amenazas consideradas para una aplicación, y consiste en el siguiente acrónimo:

- Spoofing identity (suplantación de identidad).
- Tampering (falsificación).
- Repudiation (repudio).
- Information disclosure (revelación de información).
- Denial of service (denegación de servicio).
- Elevation of privilege (escalada de privilegios).

DREAD, por su parte, es un esquema que permite priorizar las acciones para mitigar el riesgo, el cual se puede cuantificar al multiplicar la probabilidad de que la amenaza se produzca por el daño potencial

ESTRUCTURA INTERNA

Por lo general, una aplicación web se estructura en **tres capas** definidas. La primera la constituye el navegador web del lado del cliente; la segunda, un motor web capaz de usar tecnologías dinámicas en el servidor; y la tercera es la base de datos que almacena la información.

(Riesgo = Probabilidad x Daño potencial). El acrónimo significa:

- Damage potential (daño potencial).
- Reproducibility (reproducibilidad).
- Exploitability (explotabilidad).
- Affected users (usuarios afectados).
- Discoverability (descubrimiento).

LOS ESTÁNDARES UTILIZADOS

Es importante destacar que no es lo mismo una metodología que un estándar de codificación, por lo que cada equipo de desarrollo o empresa deberá determinar qué utilizar basado en prácticas comunes, o cumplir las normativas basadas en mejores prácticas.

Algunos ítems que se deben considerar son los lineamientos de la arquitectura, los niveles de documentación requeridos y los requerimientos de testeo. También se contemplan los niveles y estilos de comentarios dentro del código, el manejo de excepciones, el uso de flujo de bloques de control y la nomenclatura de variables, de funciones, de clases y de tablas. En función de éstos y otros temas se definirá la forma de escribir el software en base a los estándares existentes.

RIA: RICH INTERNET APPLICATIONS

Las **RIA**, o **Aplicaciones de Internet Enriquecidas** son aplicaciones que nacen del aprovechamiento de las ventajas de las aplicaciones web y las tradicionales. En las aplicaciones web, se recargan continuamente las páginas cada vez que el usuario hace clic sobre un vínculo, lo que produce mucho **tráfico** entre el servidor web y el navegador, teniendo que recargar todo incluso frente al menor cambio.

En las aplicaciones enriquecidas no se producen **recargas** totales por cada cambio, sino que se carga inicialmente la aplicación completa y la comunicación con el servidor solo ocurre si se necesitan datos del exterior. Además, las capacidades multimedia se mejoran fuertemente, dado que los entornos RIA cuentan con

PROVEEDORES DE SERVICIOS DE APLICACIONES

Muchos proveedores de software ofrecen acceso a sus programas por medio de Internet e incluso, a veces, adaptan aplicaciones existentes a interfaces web. Así, el usuario paga periódicamente para utilizar la aplicación, sin instalarla en ningún equipo.

reproductores internos. Entre las numerosas herramientas y tecnologías para el desarrollo de entornos RIA, se encuentran **Flash**, **Flex** y **AIR**, **OpenLaszlo**, **AJAX**, **Silverlight**, **JavaFX Script**, y **Javascript**.

CANONICALIZACIÓN INFORMÁTICA

La canonicalización en Informática (se suele abreviar como **c14n**, donde 14 representa la cantidad de letras entre la c y la n) se refiere técnicamente al proceso de **convertir datos** que tienen más de una posible representación en una estándar, **canónica**. En términos de **SEO** (*Search Engine Optimization*), implica determinar la mejor URL para mostrar de un sitio, ya que éste puede ser presentado de distintas maneras. En todas las opciones aparecería el mismo contenido, pero para un buscador no será lo mismo y produciría duplicación. Por ejemplo:

- **http://www.sitio.com/index.php**
- **http://www.sitio.com**
- **http://sitio.com**

En el servidor Apache, el uso de **`mod_rewrite`** permite redirigir de forma transparente y a nivel interno las urls definidas. El siguiente ejemplo implica que cualquier búsqueda que no corresponda a la forma **www.sitio.com** será redirigida a la correcta, con un error 301.

```
RewriteEngine on
RewriteCond %{HTTP_HOST} !^www\.sitio\.com
RewriteRule ^(.*)$ http://www.sitio.com/$1
[R=301, L]
```

Si, en cambio, hablamos de **Unicode**, las codificaciones de longitud variable tienen más de un posible código para los caracteres más comunes. Esto complica la validación por cadenas de caracteres, ya que deberían considerarse todas las posibles cadenas. Un software que no contempla todas las codificaciones corre el riesgo de aceptar cadenas consideradas inválidas. La solución es admitir un único tipo de codificación por carácter.

EL NUEVO MODELO

En 2006, Microsoft anunció **ACE Threat Analysis and Modeling v2**, la revisión de su metodología anterior, que cambia la perspectiva de análisis hacia el punto de vista de la defensa. Sus pasos de aplicación son: definición, modelización, cuantificación y validación.

Entonces, utilizamos la canonicalización para traducir cada carácter al único formato permitido. Una alternativa sería que el servidor rechazara peticiones no canonicalizadas e hiciera cargo de la canonicalización al cliente. Para obtener más información, podemos leer el RFC 2279: *UTF-8, a transformation format of ISO 10646 (***www.ietf.org/rfc/rfc2279.txt**).

WEB APPLICATION FIREWALLS

Los **WAF** (*Web Application Firewalls*) o firewalls de aplicación web son elementos que trabajan en la capa de aplicación y regulan el tráfico entre una aplicación y su entorno (servicios del SO), enfocándose al tráfico HTTP en particular.

Su principal tarea es evitar ataques basados en la manipulación de las comunicaciones HTTP y la alteración de parámetros en peticiones. Así se obtiene un mayor grado de protección al combinarlo con otros dispositivos de prevención en entornos de red (sistemas de detección de intrusos, firewalls comunes, etcétera).

Algunas regulaciones promueven que las aplicaciones web que trabajan online y están orientadas a servicios financieros cuenten con elementos de esta naturaleza. Tal es el caso de **PCI Data Security Standard**, que requiere la presencia de éstos para

Las RIA, o Aplicaciones de Internet Enriquecidas, son aplicaciones que nacen del aprovechamiento de las ventajas de las aplicaciones web y las tradicionales

DIFERENCIAS CONCEPTUALES

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

su cumplimiento. Algunos de los programas WAF más conocidos con licencia libre son **WebKnight**, de AQTronix (**www.aqtronix.com**) y **Modsecurity**, de Breach (**www.modsecurity.org**, **Figura 4**), aunque existen muchos otros comerciales.

EL ESTÁNDAR OWASP

OWASP (*Open Web Application Security Project*) es, según su propio sitio web, un proyecto de código abierto dedicado a determinar y a combatir las causas que hacen que las aplicaciones web sean inseguras.

Los documentos y proyectos más destacados de OWASP son, probablemente, la **Guía OWASP** y el documento de autoevaluación **OWASP Top 10**.

Entre las herramientas creadas, se incluye el entorno de entrenamiento **WebGoat** (**Figura 5**), la herramienta de pruebas de penetración **WebScarab** (**Figura 6**) y las utilidades para entornos .NET **OWASP DotNet**. Podemos encontrar la lista completa de herramientas en la siguiente dirección: **www.owasp.org/index.php/Phoenix/Tools**.

FIGURA 4.
Modsecurity es un módulo del servidor Apache que actúa como Web Applicacion Firewall embebible y sirve para realizar análisis en tiempo real.

HTML SCRIPTING

El lenguaje HTML puede llamar a un script y extender su potencial. Así, pueden surgir ataques de **HTML scripting**, cuyo objetivo es inyectar código de forma tal que éste sea retornado como parte de la salida de una aplicación y modifique su comportamiento normal.

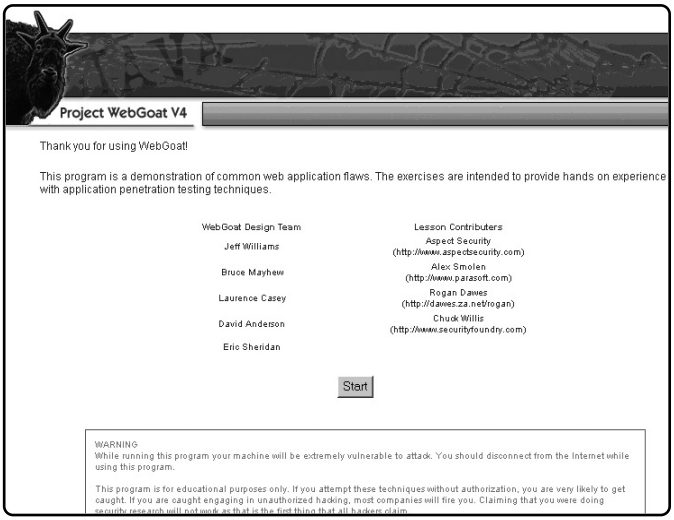


FIGURA 5.
WebGoat es una aplicación J2EE deliberadamente insegura para el aprendizaje. Cuenta con lecciones donde se debe demostrar la comprensión de problemas y también provee pistas y código de ayuda.

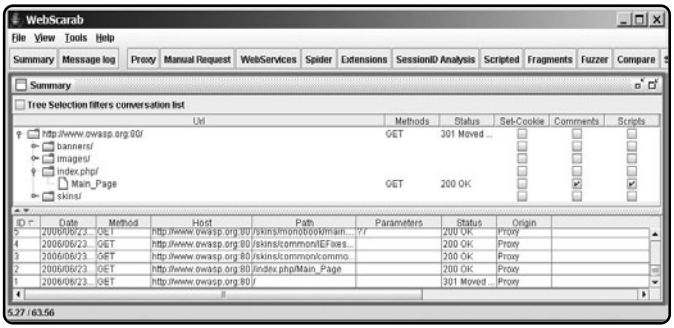


FIGURA 6.
WebScarab es una aplicación Java, que permite analizar aplicaciones web que utilicen HTTP y HTTPS. Puede trabajar en varios modos, pero el más común es el de proxy.

LA FUNDACIÓN OWASP

Es una organización sin fines de lucro, que apoya los proyectos de OWASP. La comunidad está conformada por empresas, entidades educativas y usuarios de todo el mundo, que confeccionan artículos, estándares, metodologías y tecnologías para ser usadas libremente.

Vulnerabilidades y tipos de ataque

Los ataques asociados a entornos web están relacionados con una gran **superficie de ataque** y diversas maneras de encarar un plan de reconocimiento, análisis y penetración. Esto se debe a que son muchos los componentes implicados en el universo web, desde las bases de datos, los distintos lenguajes y tecnologías, los propios servidores web y otros componentes.

RECOPILACIÓN DE INFORMACIÓN

La recopilación de información se basa principalmente en la **identificación** del servidor y la aplicación web, y utiliza técnicas conocidas de identificación TCP/IP, pero orientadas al nivel de aplicación.

Se intenta crear un **perfil** del objetivo, configuraciones y arquitectura de red, analizando distintos elementos, como los resultados de respuestas y cabeceras HTTP, archivos de extensiones conocidas, cookies, páginas por defecto y de error, estructuras y convenciones de directorio, interfaces de administración, etcétera.

Con esta información, se desarrolla un escenario de ataque específico. La exactitud es fundamental ya que muchas vulnerabilidades son dependientes de un software y versión específicos, por lo que un servidor o aplicación web que se identifica de manera obvia, no ayuda a la seguridad.

ABUSO DE FUNCIONALIDADES

Esta técnica aprovecha las características propias y funcionalidades de un sitio o aplicación web para

La recopilación de información se basa principalmente en la identificación del servidor y la aplicación web

EL RFC DE HTTP

El **RFC 2068** impulsa a los administradores web a ocultar la versión de software en su cabecera **server**, indicando: *La revelación de la versión de software del servidor permite que sea más vulnerable a ataques contra el software del que se conocen agujeros de seguridad.*

obtener beneficios sin estar autorizado o producir un comportamiento no esperado. Las técnicas de abuso se combinan con otras categorías de ataques y convierten las aplicaciones con un propósito útil en herramientas para propósitos maliciosos.

Algunos ejemplos podrían ser el uso de la función de búsqueda de un sitio para acceder a archivos restringidos, el engaño del mecanismo de subida de archivos para reemplazar archivos críticos, la denegación de servicios de autenticación para bloquear a los usuarios válidos y la modificación de los precios en un carrito de compras online.

ATAQUES DE INYECCIÓN

La inyección de código implica la explotación de una vulnerabilidad causada por el procesamiento de datos no válidos, y puede ser utilizada para cambiar un comportamiento o flujo de ejecución. Se relacionan con datos de entrada asumidos equivocadamente y el desconocimiento de sus efectos, y se aplica tanto a entornos web como a programas binarios y librerías. Para realizar estos ataques, es común emplear un **proxy local** que capture las transacciones entre el navegador y el servidor web, para que puedan ser manipuladas antes de salir del sistema, lo cual saltea la protección de una interfaz bien diseñada que limite el ingreso de datos de usuario.

Como protección, se deben usar métodos seguros de entrada y salida de datos (sin olvidar las **validaciones**), evitar caracteres peligrosos, codificar los datos y utilizar buenas prácticas de programación.

Los ataques de XSS **reflejados** se producen cuando los datos provistos por un cliente web son usados del lado del servidor para producir resultados del lado del usuario. Si éste ingresa datos sin ser validados, podría ocurrir que ese código fuera incluido en la página generada dinámicamente. Esto también puede darse en forma local e incluso otros archivos HTML pueden presentar problemas de XSS, que no se limita a la extensión .htm o .html, pudiendo ser archivos **CHM** (*Compiled Help Module*) de ayuda o templates, por ejemplo.

LAS APLICACIONES SEGURAS

Se considera correcto tener en cuenta la seguridad desde el inicio, tener políticas documentadas, una metodología de desarrollo con controles adecuados y una correcta gestión de versiones y configuración.

XSS (Cross Site Scripting)

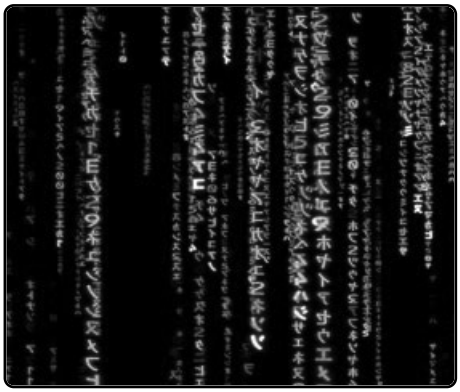
IMPLICANCIAS DEL CROSS SITE SCRIPTING

La criticidad del XSS radica en que el navegador procesa un script enviado por el propio servidor, originado en la aplicación al que hizo la petición. Estos ataques habilitan acciones que, en condiciones normales, estarían prohibidas, como Cookie Access, Object Model Access, User Data Access, Bypassing SiteLock restrictions y Zone Elevation.

ENLACES CON INFORMACIÓN SOBRE XSS

Algunos recursos web interesantes:

- HTML Scripting Attack de H. Racciatti (**www.slideshare.net/ seguinfo/ racciatti-html-scripting-attacks**)
- Malicious HTML Tags Embedded in Client Web Requests (**www.cert.org/advisories/ CA-2000-02.html**)
- The Cross Site Scripting FAQ (**www.cgisecurity.com/articles/ xss-faq.shtml**),
- Cross Site Scripting Info (**http://httpd.apache.org/ info/css-security**)



Un escenario de ejemplo podría ser el siguiente: un atacante envía un e-mail con el enlace a un sitio vulnerable. La víctima accede y un script enviará, a otro equipo controlado por el atacante, las cookies de la víctima y de todos los que accedan. Otro ejemplo podría ser un atacante que envía a la víctima un e-mail con un enlace a una página manipulada para aprovechar un bug local. Al acceder, se abre el archivo vulnerable y el script malicioso puede ejecutar comandos en el equipo de la víctima, con sus privilegios (**Figura 7**).

En su funcionalidad, los ataques de XSS **persistentes** son similares a los ataques reflejados, pero los datos del atacante quedan almacenados en el servidor. En lugar de hacer que la víctima realice una petición que contiene el script, el atacante lo almacena y espera que la víctima visite el sitio y lo ejecute. Si los datos brindados y devueltos a un usuario son almacenados por la aplicación sin correcta validación, a diferencia del XSS reflejado podría darse que el código fuera ejecutado con cada visualización (por ejemplo, foros y redes sociales).

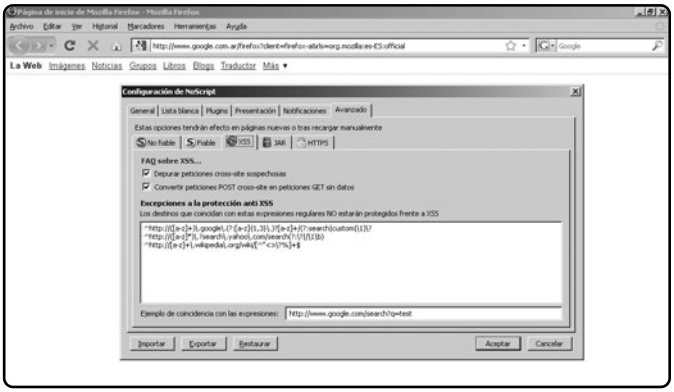


FIGURA 7.
NoScript es un plugin para Firefox, que permite evitar todo tipo de scripts y protegerse de ataques del tipo XSS y clickjacking.

Algunas contramedidas generales son, por ejemplo, minimizar los ingresos en formulario, codificar los datos y crear una capa entre la entrada de datos y el **backend**, para evitar la inyección directa.

Web 2.0 y nuevas tecnologías

Si hay una cosa que podría superar la velocidad a la que avanza la tecnología, es la velocidad a la que avanza la tecnología. Esto no es paradójico en absoluto, ya que cada día se tarda menos en alcanzar el

APLICACIONES SUSCEPTIBLES

Muchas aplicaciones pueden ser potenciales víctimas de un ataque de XSS. Los principales tipos de sistemas web susceptibles son los blogs, las salas de chat, los libros de visitas, los clientes de webmail, los formularios de confirmación y los foros.

siguiente escalón. En otras épocas, los cambios demoraban años y a veces siglos, pero en la última mitad del siglo XX, se superó en muy poco tiempo todo lo conocido por el ser humano, y el cambio fue tan vertiginoso que solo quedó la opción de subirse a la ola y navegarla. La tecnología no fue la excepción a esta tendencia, tomando aun más protagonismo a partir del período mencionado.

Si nos centramos en la última década, Internet se viene perfilando implacablemente como el factor de cambio por excelencia, dado todo lo que hoy en día es dependiente de la red. Y es que la globalización ha reducido nuestra percepción del tamaño del mundo, haciendo que cada nuevo dato esté disponible para todos en el menor tiempo imaginado. Lo que ocurre hoy es que hay, tal vez, demasiadas cosas, demasiadas opciones, problemas y soluciones para lo mismo (**Figura 8**).

FIGURA 8. Tim Berners Lee es considerado el creador de la World Wide Web y, actualmente, es el director del Consorcio Internacional W3C.

FIGURA 9. Así lucía el sitio web de Google en Diciembre de 1998, una época sin demasiadas tecnologías existentes y muy lejos de la Web 2.0.

LA FUGA DE INFORMACIÓN

Es un problema que se produce cuando un sitio web revela datos sensibles, como los comentarios del desarrollador o mensajes de error, que pueden ayudar a un atacante a explotar el sistema. La fuga no representa necesariamente una brecha de seguridad.

ESTÁNDARES CAMBIANTES Y SU SEGURIDAD

Nunca se anunció una Web 1.0 (**Figura 9**), pero un día nos encontramos con una versión 2.0 (**Figura 10**), tal vez sin darnos cuenta de que estábamos avanzando. Antes, solo existía el producto maduro del concepto original, con páginas estáticas y sin demasiada actualización. Pero el público consumidor comenzó a dirigirse hacia sitios de mayor interacción, personalizados, visualmente más agradables.

FIGURA 10. Mapa de servicios Web 2.0 elaborado por la gente de Internality (www.internality.com), que podemos descargar en distintos formatos.

LA PALABRA DE UN GURÚ

Podemos decir que cada vez dependemos más de cosas que entendemos menos. En palabras del genial **Bruce Schneier**: *si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología.*

Datos útiles sobre la Web 2.0

EL BAUTISMO DE LA WEB 2.0

El creador del concepto de Web 2.0 fue Tim O'Reilly en el año 2004, para definir a la segunda generación histórica de la World Wide Web. Esta nueva Web estaría basada en comunidades virtuales, servicios y entornos colaborativos, como las redes sociales, los blogs, las wikis y los demás sistemas que promueven la interacción entre las personas y el intercambio de información.

WEB 2.0 Y WEB SEMÁNTICA

Algunos enlaces con información muy interesante son:

- Mapa visual de la Web 2.0 (**http://internality.com/web20**)
- Web 2.0 Summit (**www.web2summit.com**)
- Qué es la Web 2.0 (**www.microsoft.com/spain/empresas/internet/web_2.mspx)**
- Guía breve de la Web Semántica (**www.w3c.es/Divulgacion/Guiasbreves/WebSemantica**)

El mercado respondió con la mejora de sus tecnologías, que por la forma que ha tomado se dice que es una versión **beta constante**.

Nos referimos a Web 2.0 cuando hablamos de servicios que utilizan distintos recursos y cuyo contenido y presentación pueden ser modificados por los usuarios. Tiene una infraestructura propia y se puede decir que un sitio es de tecnología Web 2.0 si emplea, en alguna medida, componentes como **CSS**, **microformatos**, **AJAX**, **JavaScript**, **RSS**, soporte para posts, **XML**, **mashup** y otras similares (**Figura 11**).

Entre los nombres más escuchados tenemos **AJAX** (*Asynchronous JavaScript And XML*), que es un conjunto de tecnologías que permite realizar peticiones de fragmentos de contenidos desde el servidor, dando así mayor velocidad y disponibilidad al trabajar sin interrupciones ni recargas completas de una página. Las aplicaciones basadas en AJAX son muy transparentes, pero el cliente recibe mucha información acerca de cómo funcionan, lo que las hace ideales para **ingeniería inversa**.

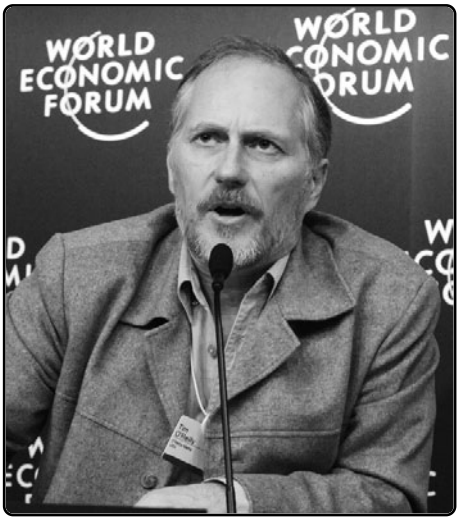


FIGURA 11. Tim O 'Reilly**, fundador y presidente de O'Reilly Media e impulsor del software libre, fue uno de los autores del concepto Web 2.0.**

Se dice que la Web 2.0 requiere una **Seguridad 2.0**, pero no sabemos si aun estamos preparados para ella y aquí hay un choque de ideas: la tendencia indica una mayor facilidad de uso y operabilidad, en tanto que la seguridad siempre atenta contra éstas.

Es posible lograr un equilibro incorporando la seguridad como parte de los procesos iniciales de desarrollo. La ecuación **seguridad versus comodidad** solo existe al considerar la primera como elemento externo molesto que se incorpora al final.

Se dice que la Web 2.0 requiere una Seguridad 2.0, pero no sabemos si aun estamos preparados para ella

RESUMEN

En este capítulo, hemos analizado los componentes y protocolos relacionados con la Web, así como también algunas tecnologías y lenguajes utilizados. Además, hablamos de las aplicaciones web, de los problemas que pueden encontrarse en ellas y de algunas vulnerabilidades.

Multiple **choice**

1 ¿Cómo se llaman los elementos que trabajan en la capa de aplicación y regulan el tráfico entre una aplicación y su entorno?

a- AJAX
b- XSS
c- Firewall de aplicación Web
d- Backend

2 ¿Cómo se llama la técnica que permite la explotación de una vulnerabilidad causada por el procesamiento de datos no válidos?

a- Encoding
b- RIA
c- OSWAP
d- Ataques de inyección

3 ¿Qué es el header monitor?

a- Un lenguaje de programación.
b- Un protocolo de transferencia.
c- Un plugin de Firefox que muestra el estado de respuestas del protocolo HTTP.
d- Un honeypot.

4 ¿Cómo se llama la técnica que permite convertir un carácter de un lenguaje natural en un símbolo de otro sistema de representación mediante la aplicación de reglas?

a- Encoding
b- RIA
c- OSWAP
d- Ataques de inyección

5 ¿En dónde trabaja el protocolo HTTP?

a- XML
b- Puerto TCP 80
c- Mashup
d- ASP

6 ¿Cómo se llama la técnica de convertir datos que tienen más de una posible representación en una estándar?

a- Encoding
b- Sniffing
c- Canonicalización
d- 2005

Respuestas: 1-c, 2-b, 3-c, 4-a, 5-d, 6-c.

Capítulo 6

Infraestructura de redes

En este capítulo, analizaremos distintos aspectos de la seguridad en infraestructura de redes.

Infraestructura de redes

En este capítulo, abordaremos la temática de las redes de comunicaciones. Introduciremos algunos conceptos de técnicas de ataque que, combinadas, dan lugar a ataques más complejos. Por otro lado, haremos referencia a las distintas tecnologías y dispositivos de seguridad, para finalmente abordar un tema que cada vez tiene mayor relevancia: las redes inalámbricas y su seguridad.

Técnicas de ataque

Muchas de las técnicas que analizaremos a lo largo de este capítulo tienen varios años de desarrollo, incluso décadas, y sentaron las bases de ataques más complejos. Muchas de esas acciones son meramente conceptuales, por lo que pueden ser adaptadas a innumerables escenarios, no solamente enmarcadas dentro de las redes informáticas o de comunicaciones.

Las técnicas que veremos a continuación son: la **escucha de protocolos** o **sniffing**, **impersonalización** o **spoofing**, **envenenamiento** o **poisoning**, el **robo de sesiones** o **hijacking** y finalmente el **consumo** o **saturación de recursos**.

ESCUCHA DE PROTOCOLOS: SNIFFING

Un **sniffer** o analizador de protocolos es una aplicación utilizada para **monitorear** y **analizar** el tráfico en la red. Permite capturar el tráfico y examinarlo en función de los protocolos soportados, aplicando distintos tipos de filtros. También es muy usado para detectar errores y problemas de diseño en las redes.

Con este tipo de aplicaciones, es posible obtener datos sin problemas, si es que son transmitidos en **texto plano**. Por lo tanto, cualquier protocolo que envíe los datos de esta forma es susceptible de ser analizado por un sniffer. Dentro de estos protocolos, tenemos ejemplos como **HTTP**, **SMTP**, **POP3**, **IMAP**,

EL LLANTO DEL SNIFFING

Si alguna vez hemos leído historietas, habremos observado que, cuando se representa a uno de los personajes llorando, se utiliza algo como *snif-snif*. Esto no es una onomatopeya sino que en inglés significa **sorber** o **inhalar** por la nariz, acto que se produce al llorar.

Un sniffer o analizador de protocolos es una aplicación utilizada para monitorear y analizar el tráfico en la red

Telnet, **FTP**, etcétera. Para lograrlo, el sniffer configura la placa de red en un estado conocido como **modo promiscuo**, en el cual en la **capa de enlace de datos** del modelo OSI se conservan las tramas no destinadas a la dirección MAC de dicha placa. De esta manera, se puede capturar todo el tráfico que pasa por cualquier dispositivo conectado a la red.

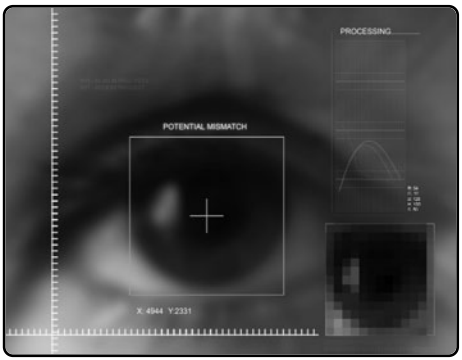
El uso de un switch dentro de una red sería una limitación, ya que en este caso aunque la placa de red esté en modo promiscuo, el switch es quien reenvía los paquetes únicamente al destino que corresponde. De todas formas, al aplicar la técnica de **ARP poisoning**, esta limitación puede sortearse con relativa facilidad.

De acuerdo con nivel de interacción que el sniffer tenga con la red al momento de la captura del tráfico, podremos diferenciar entre técnicas de **sniffing pasivas** y **sniffing activas**. En las primeras, también denominadas **eavesdropping** (aunque en rigor de verdad esta técnica no se acota al sniffing de paquetes de red), el sniffer solo se limita a escuchar el tráfico que circula por determinado segmento, sin enviar ningún tipo de paquete. Suele colocarse en segmentos de alto tráfico, como por ejemplo los *backbones*.

Dado que no envía paquetes a la red, este tipo de sniffers no es apto para redes segmentadas por switches ya que, como veremos, el ataque de ARP poisoning requiere enviar una serie de paquetes ARP.

Los sniffers activos actúan enviando paquetes especialmente generados para diversos fines. Debido a que generan tráfico, no monitorean todo un segmento sino que son colocados en puntos estratégicos, escogiendo específicamente los equipos que se van a analizar, para evitar sobrecargas en la red.

Como mencionamos, las aplicaciones que implementan la técnica de sniffing son los analizadores de



protocolos (**Figura 1**). A continuación, mencionaremos y detallaremos brevemente los más conocidos.

En primer lugar, quizás el más famoso de ellos sea **Wireshark**, anteriormente conocido como **Ethereal**, utilizado para analizar y detectar problemas en redes de comunicaciones y como una herramienta didáctica. Cuenta con todas las características estándares de un analizador de protocolos. Permite ver la totalidad del tráfico que pasa a través de una red, usualmente Ethernet, aunque es compatible con otras, configurando la placa de red en modo promiscuo.

Algunos de los atributos más sobresalientes de **Wireshark** es el hecho de que está liberado bajo licencia GPL, posee una interfaz intuitiva, capacidades de filtrado ricas y flexibles, soporte para formato estándar de archivos **tcpdump**, la posibilidad de reconstruir sesiones TCP, es multiplataforma, etcétera.

Aunque no posee la interfaz gráfica de Wireshark, **tcpdump** es una herramienta de línea de comandos cuyo principal objetivo es analizar a bajo nivel el tráfico que circula por la red. Permite al usuario capturar y mostrar en tiempo real los paquetes transmitidos y recibidos en la red a la cual el equipo está conectado.

Funciona en la mayoría de los sistemas operativos del tipo UNIX, en los cuales hace uso de la librería **libpcap** para la captura de paquetes. Brinda la posibilidad de aplicar varios filtros para obtener una salida más depurada. Sin éstos, tcpdump vuelca todo el tráfico que pase por la placa de red elegida (**Figura 2**).

El tercero en cuestión es **Ettercap**, que permite realizar sniffing activo y pasivo de varios protocolos, incluso aquellos cifrados, como SSH (versión 1), por ejemplo (**Figura 3**). También hace posible la inyección de datos en una conexión establecida y el filtrado en

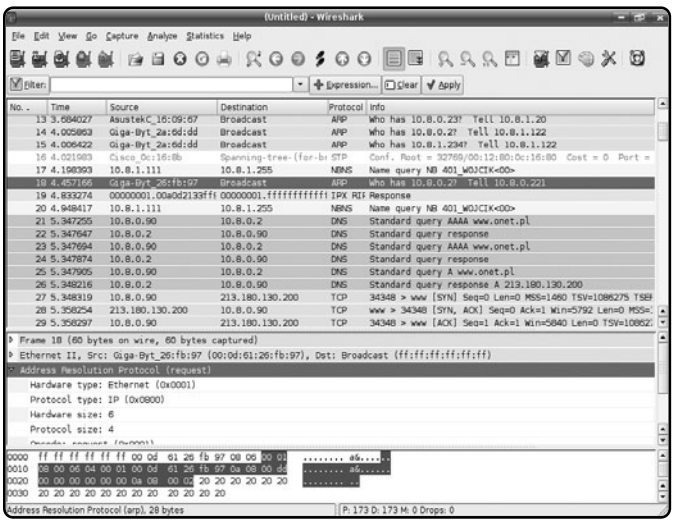


FIGURA 1.
Ejemplo de visualización del tráfico de una red Ethernet con Wireshark. Es importante notar cómo quedan discriminados los distintos protocolos.

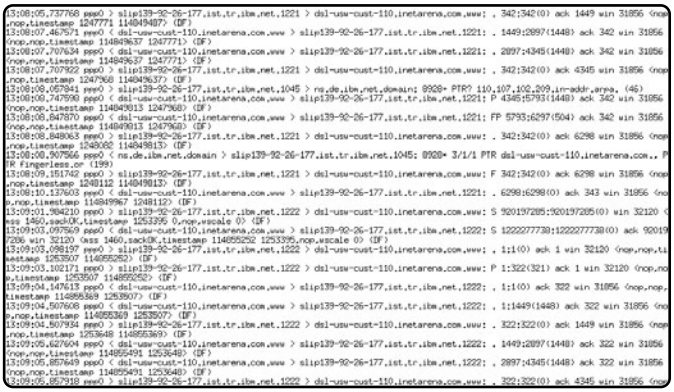


FIGURA 2. Tráfico de red con tcpdump. Podemos ver el host y los puertos de origen y destino de las conexiones.

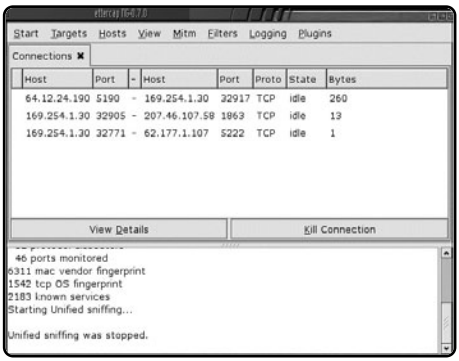


FIGURA 3. Tráfico de red que podemos observar con una versión con interfaz gráfica de Ettercap. En la ventana inferior, aparece el progreso del análisis.

tiempo real, aun manteniendo la conexión sincronizada, dado que permite implementar ataques **Man-in-the-middle**.

Un sniffer particular es **Kismet**, ya que está orientado a las conexiones inalámbricas 802.11 (**Figura 4**). Funciona con cualquier placa wireless que tenga soporte para **modo monitor** (el modo monitor de WiFi es el equivalente al modo promiscuo en redes Ethernet) y permite rastrear tráfico de diversas normas. Se diferencia de la mayoría de los otros sniffers inalámbricos en su funcionamiento pasivo, es decir que lo hace sin enviar ningún paquete detectable. También incluye características básicas de detección de intrusos, por ejemplo, la detección de programas

MODO PROMISCUO

El protocolo Ethernet reenvía todos los paquetes a todos los dispositivos de un mismo segmento de red. Cuando una placa tiene habilitado el modo promiscuo, no solo capturará el tráfico que está destinado a ella, sino todo el de ese segmento.

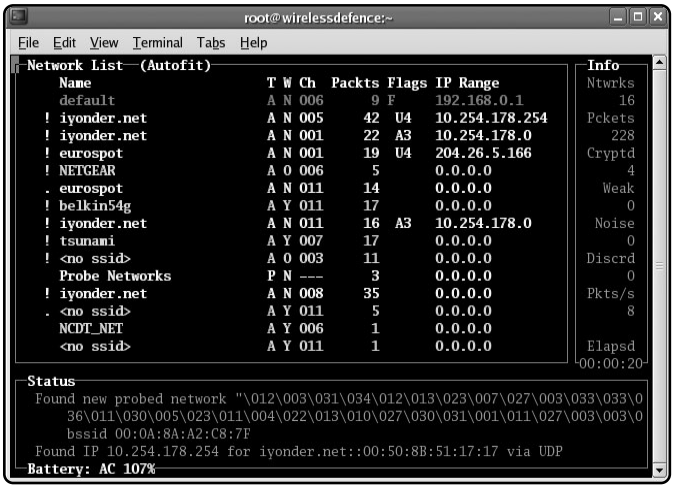


FIGURA 4.
Tráfico de una red wireless con una versión con interfaz gráfica de Kismet, donde puede verse el detalle de todas las redes inalámbricas detectadas.

de rastreo inalámbricos como **NetStumbler**, así como ciertos ataques a redes inalámbricas, y corre bajo gran cantidad de plataformas basadas en UNIX.

Finalmente, en el caso de plataformas Microsoft, un sniffer con gran cantidad de funcionalidades es **Cain & Abel** (**Figura 5**). Es una herramienta de análisis de protocolos que, además, permite la recuperación de contraseñas para plataformas Microsoft, la cual aprovecha las fallas de seguridad de algunas implementaciones de nuevos protocolos y métodos de autenticación.

En la siguiente dirección, **www.segu-info.com.ar/articulos/17-escucha-mensajes-privados.htm**, podemos leer un interesante artículo sobre sniffing.

IMPERSONALIZACIÓN: SPOOFING

El **spoofing** es una técnica utilizada para **suplantar la identidad** de otro sujeto, que puede ser un usuario, un proceso u otro (**Figura 6**). Dependiendo del protocolo al que se haga referencia, esta técnica se implementará de diversas maneras, aunque las más utilizadas son las de **ARP spoofing** e **IP spoofing**.

HERRAMIENTAS

Ettercap: **http://ettercap.sourceforge.net**, Kismet: **www.kismetwireless.net**, Cain & Abel: **www.oxid.it**, HTTPTunnel: **www.http-tunnel.com**, Specter: **www.specter.com**, KFSensor: **www.keyfocus.net/kfsensor** y Wireshark: **www.wireshark.org**,

Otras aplicaciones de esta técnica son: **DNS spoofing**, **Web spoofing**, **e-mail spoofing** y un largo etcétera. En términos generales, podemos englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad. El IP spoofing consiste en sustituir la dirección IP de origen de un paquete TCP/IP por otra dirección IP a la cual se le desea suplantar la identidad.

Esto se consigue con programas que implementen esta técnica y es aplicable a cualquier protocolo contenido por TCP/IP, por ejemplo, ICMP, UDP o TCP. Es importante tener presente que las respuestas del host que reciba los paquetes irán dirigidas a la dirección IP falsificada. Por ejemplo, si se envía un ping *spoofeado*, la respuesta será recibida por el host al que pertenece realmente la IP.

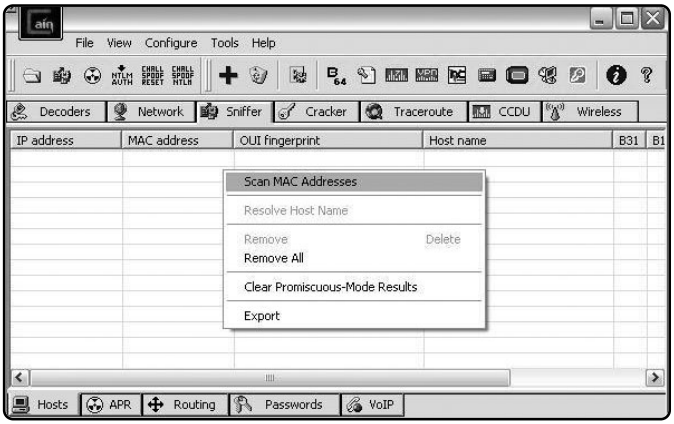


FIGURA 5.
Preparación de un análisis con la aplicación Cain & Abel.

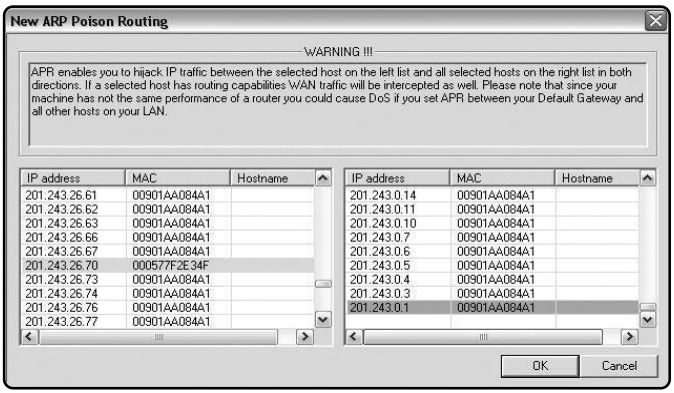


FIGURA 6.
Ejemplo de ARP Spoofing con Cain & Abel.

En el caso del MAC spoofing, existen razones muy diversas para decidir modificar la dirección MAC de un dispositivo de red. En primera instancia, una pregunta que surge es ¿cómo es posible cambiar la dirección MAC de un dispositivo si está grabada en una memoria de solo lectura que no permite ser modificada?

La respuesta es simple: si bien es cierto que dicha memoria no puede variarse, también es real que los distintos sistemas operativos no consultan directamente al hardware, sino que lo hacen a través del correspondiente controlador. Es decir, la dirección MAC es leída y almacenada por el controlador, lo que posibilita modificarla desde ese lugar.

Al depender del controlador, la forma de modificarla de acuerdo con cada sistema operativo, con comandos propios del sistema (en el caso de Linux y todos los *NIX) o con el cambio de algunas cadenas del registro (en el caso de Windows) es posible realizarlo sin demasiadas complicaciones.

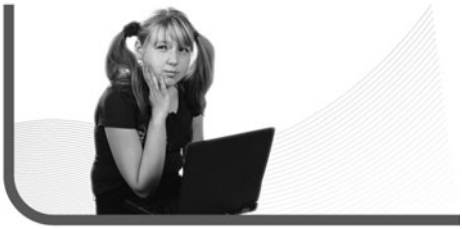
ROBO DE SESIONES: HIJACKING

El concepto de **hijacking** proviene de la palabra inglesa que significa **secuestro**. En el ámbito tecnológico, hace referencia a toda técnica ilegal que conlleve el secuestro o robo de información y sesiones por parte de un atacante. Por otro lado, se utiliza en combinación con otras técnicas y ataques, como por ejemplo, spoofing y Man-in-the-middle.

Su aplicación es muy amplia y puede puntualizarse en varias técnicas específicas. Podemos hablar del secuestro de conexiones de red o sesiones de terminal (**session hijacking**), servicios, módems, páginas (**page hijacking**) e incluso últimamente existen variantes como el secuestro del portapapeles o **clipboard hijacking**, donde el portapapeles es capturado y cada vez que se intenta pegar lo que se debería encontrar en él, aparece una URL con una dirección maliciosa. Otro nuevo ataque de similares características es el **clicjacking** o secuestro de los clics del mouse.

PROTOCOLO ARP

ARP (*Address Resolution Protocol*) es el protocolo responsable de encontrar la dirección MAC que corresponde a una determinada dirección IP. Cada máquina mantiene una tabla con las direcciones traducidas para reducir las demoras y la carga.



El concepto de hijacking proviene de la palabra inglesa que significa secuestro

Entre las técnicas más conocidas está el **session hijacking** o **secuestro de sesión**, que consiste en un atacante que toma el control de una conexión TCP/IP, por ejemplo durante una sesión Telnet y le permite inyectar comandos o realizar un ataque de DoS. Una evolución de esta práctica sería, a partir de una sesión autenticada, tomar las credenciales de una de las partes y luego adueñarse de la sesión como si fuera el cliente válido.

Otro de los usuales ataques es el **browser hijacking** o secuestro del navegador. Se denomina de esta manera a la apropiación que realizan algunos tipos de malware, en particular spyware, sobre el navegador web, al lanzar pop-ups, al modificar la página de inicio, al cambiar la página de búsqueda predeterminada, etcétera.

El caso del **page hijacking** o secuestro de un sitio web hace referencia a las transformaciones que un atacante realiza sobre una página web, normalmente explotando alguna vulnerabilidad en el servidor o aprovechando un bug de programación del sitio web.

La técnica de **módem hijacking** o secuestro del módem es la que era utilizada por un tipo de malware llamado **dialers**, muy común cuando la conexión por dial up todavía era un estándar. Los dialers eran pequeñas aplicaciones maliciosas que, sin el consentimiento del usuario, creaban y configuraban conexiones a números de servicios especiales.

CONSUMO MASIVO DE RECURSOS: FLOODING Y DDOS

En esta sección, analizaremos distintas técnicas y ataques que tienen como objetivo **saturar** determinados **recursos** de un sistema.

La primera que trataremos es **IP flooding**, que se basa en saturar (**inundar**) determinado servicio

MENSAJES DEL PROTOCOLO ARP

Cuando un host quiere comunicarse con una IP, emite un paquete **ARP-Request** a la dirección de Broadcast y le solicita la dirección MAC del host. El equipo con la IP pedida responde un paquete **ARP-Reply** y le indica su MAC.

de red mediante el envío de paquetes IP. Los ataques que implementan esta técnica pueden utilizarse para bajar el rendimiento de la red a la cual está conectado el atacante y generar paquetes con origen y destino aleatorio. Además de esto, también puede buscarse como objetivo saturar los recursos de red de una víctima en particular, para después poder llevar a cabo un ataque de session hijacking, entre otros posibles. Una forma de potenciar los resultados de esta técnica es utilizar la dirección de broadcast.

Esta evolución del IP flooding lleva el nombre de **Broadcast IP flooding**, ya que se basa en enviar paquetes IP a dicha dirección. A continuación, analizaremos dos ataques que implementan esta técnica: el ataque **smurf** y el ataque **fraggle**.

El ataque smurf emplea paquetes ICMP echo-request con la dirección IP de origen de la máquina que será atacada y con la dirección IP destino de la dirección de broadcast de la red local o de las redes que se utilizarán para atacar a la víctima. Esto hace que todos

los intermediarios reciban la petición y le respondan con paquetes ICMP echo-reply, magnificando el ancho de banda consumido y ralentizando la red hasta, incluso, con la saturación del el equipo de la víctima.

El ataque fraggle es similar al smurf, pero usa el protocolo UDP. El resultado de esta acción es que los host que tengan activo el servicio **echo** reenviarán el paquete a la víctima y los que no mandarán un ICMP de error.

El **MAC flooding** es una técnica que está orientada a atacar el switch. Éstos mantienen una tabla denominada **CAM** (*Content Addresseable Memory*), la cual relaciona direcciones MAC de los equipos de la red con el correspondiente puerto del switch. Esto es lo que le permite, junto a la tabla ARP, enviar los paquetes solo al equipo que los tiene como destino y no en forma de broadcast como lo hacen los HUBs. Un ataque de MAC flooding envía una serie de paquetes directo al switch, los cuales contienen diferentes direcciones MAC de origen. Su objetivo es consumir la memoria asociada a la tabla CAM.

El ataque orientado a consumir recursos, por excelencia, es el **DoS** (**denegación de servicio**), el cual es

El ataque orientado a consumir recursos, por excelencia, es el DoS (denegación de servicio)

una acción iniciada por un sujeto que busca saturar algún tipo de recurso, ya sea hardware, software o ambos dentro de un determinado sistema. Estos recursos son memoria, capacidad de procesamiento del CPU, conexiones de red, disco duro, etcétera. Este tipo de acciones puede clasificarse en ataques **preprogramados** y ataques por **control remoto**. En el caso de los ataques preprogramados, se utiliza algún tipo de malware (usualmente un **worm**) que va contagiando a otros sistemas y luego implementa un ataque de DoS al cumplirse una determinada condición de tiempo. En el caso de los ataques por control remoto, éstos usan equipos comprometidos, comúnmente con un **troyano**, para realizar ataques de denegación de servicio contra cualquier IP.

Si ampliamos el concepto de DoS, cuando se realiza una acción de este tipo lanzada desde numerosos equipos, se está en presencia de un ataque de **Denegación de servicio distribuida** o **DDoS** (*Distributed Denial of Service*). Normalmente utiliza una estructura por capas, donde el atacante se conecta a servidores maestros, que son otros sistemas previamente comprometidos por él.

Cada uno de ellos controla un conjunto de host esclavos o **zombies**, que se usarán para realizar los ataques de DoS. Una vez que el máster ha sido infectado por el atacante, éste tratará de infectar otros equipos dentro de la misma red como esclavos, a partir de rutinas automatizadas para explotar vulnerabilidades en programas que acepten conexiones remotas. Las redes formadas por estos equipos comprometidos son denominadas **botnets**.

El término botnet hace referencia a una colección de distintas aplicaciones que funcionan en forma autónoma, preprogramadas por el atacante. El objetivo de este tipo de redes, por lo general, está relacionado, además de los ataques de denegación de servicio distribuida, con el envío de spam y la descarga de material ilegal, para luego ser utilizada como servidor alternativo (**Figura 7**).

HONEYPOTS

Se podría caracterizar a un **honeypot** como un elemento informático con la intención de atraer atacantes reales simulando ser sistemas vulnerables.

ROAMING

El roaming permite a distintos equipos cliente moverse libremente por una red sin perder conexión, incluso cuando dentro de ella se cambie de punto de acceso. Además, en las redes celulares, también se aplica este concepto cuando se cambia de antena con el servicio.

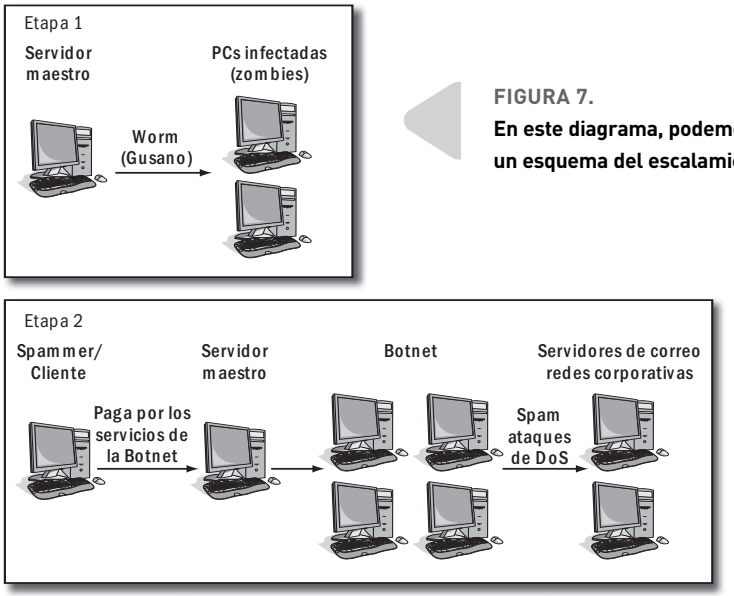


FIGURA 7.
En este diagrama, podemos observar un esquema del escalamiento de una Botnet.

Se emplea como una herramienta de seguridad informática para recoger información sobre los agresores y sus técnicas, y también puede usarse para distraerlos de los equipos más importantes del sistema. Algunos son programas que emulan sistemas operativos, pero otros son sistemas reales configurados para tal fin.

Entre las ventajas de esta aplicación podemos citar: la ausencia de falsos positivos; los bajos recursos que se necesitan para implementarlo; su funcionamiento tanto para atacantes internos como externos y fundamentalmente la poca, pero de gran valor y utilidad, recolección de información, ya que son datos tomados directamente del accionar de los agresores. Como un aspecto negativo, podemos mencionar que si no es atacado, es un recurso que está siendo desperdiciado. Por otro lado, en caso de ser realmente comprometido, de acuerdo con el tipo de honeypot que sea, es una fuente potencial de riesgo para la red de la organización.

Según el nivel de interacción del honeypot, es decir, cuán real sea, se los puede clasificar en honeypot de

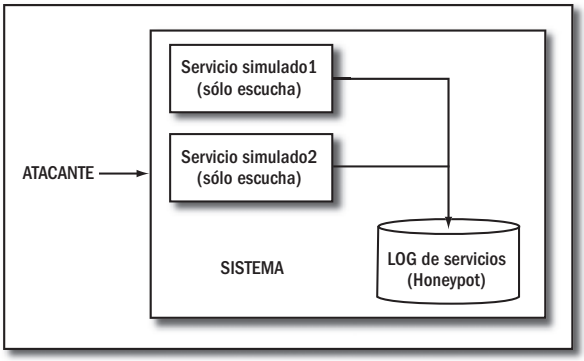


FIGURA 8. Representación de la interacción entre un honeypot de compromiso bajo y el atacante.

baja, de **media** o de **alta interacción**. Los de baja interacción o **low involvement honeypots** tienen la característica de simular solamente los puertos y servicios que se están brindando. En este caso, no existe interacción con el atacante. Por este motivo, el riesgo asociado a tener este tipo de honeypot online es mínimo, pero como contrapartida su aprovechamiento es pobre, ya que no permite la posibilidad de investigar las técnicas de los atacantes (**Figura 8**).

Se podría caracterizar a un honeypot como un elemento informático con la intención de atraer atacantes reales simulando ser sistemas vulnerables

Los honeypots de media interacción o **medium involvement honeypots** son sistemas que imitan la existencia de uno o varios servicios de forma más sofisticada. Se pretende captar la atención del atacante y permitir un grado mayor de interacción, de forma tal que facilite el análisis, aunque mínimamente, de su comportamiento. En este caso, el grado de riesgo aumenta moderadamente, ya que por un lado el servicio sigue siendo una simulación, lo que posibilita tener acotada la interacción entre el atacante y el servicio; pero por otro lado, si existe un fallo en la implementación del servicio simulado, el atacante podría aprovecharlo para atacar el sistema real.

Finalmente, los honeypots de alta interacción o **high involvement honeypots** son aquéllos sistemas que no emulan, sino que utilizan un entorno real con servicios verdaderos. Estos honeypots llaman la atención del atacante, ya que el equipo en principio está operativo y brinda servicios, lo cual permite un estudio completo de su comportamiento.

Deben estar constantemente monitoreados, ya que si un atacante logra acceder puede disponer de todo el sistema e incluso pivotear a otros puntos de la red interna que estuviesen interconectados.

También podrían utilizar el honeypot para realizar ataques a otros equipos conectados a Internet, por ejemplo, usándolo como parte de una botnet. De esta manera, concluimos que ya no podemos considerar sus logs como fuente de información confiable, por lo que debemos complementarlo con un monitoreo externo.

En Internet podemos encontrar varias herramientas que implementan los distintos tipos de honeypots que comentamos. Estas aplicaciones son muy flexibles y permiten la total configuración de servicios e incluso las vulnerabilidades a simular. Además, algunas permiten escoger el tipo de sistema operativo y la versión que se desea imitar (Solaris, Linux, Windows, etcétera).

La ubicación de los honeypots es un aspecto que no podemos descuidar. Cuando lo instalamos como medio de recopilación de información, debemos tener en cuenta que si su ubicación es demasiado obvia, cualquier atacante la descubrirá y evitará todo contacto. Para darle mayor nivel de realismo, es conveniente que esté integrado al resto del sistema, pero hay que recordar que de esta forma el riesgo de que la red sea comprometida aumenta notablemente.

El objetivo de los honeypots es obtener información de primera mano, directamente de los avezados atacantes, ya que muchas de las técnicas que pueden llegar a utilizar son desconocidas.

Desde el punto de vista de la red, podrían encontrarse tanto detrás como delante del firewall, o bien como parte de la **DMZ** (*Demilitarized Zone*).

Redes inalámbricas

Dentro de las telecomunicaciones, debemos mencionar la importancia que hoy en día tienen las **redes inalámbricas**, en particular las denominadas redes WiFi. Si bien en este apartado nos enfocaremos en éstas, debemos tener en cuenta que cada vez están tomando más relevancia otras tecnologías, como por ejemplo, **Bluetooth** y redes inalámbricas de mayor envergadura, como la red **3G**.

Antes de continuar, aclararemos que no es el objetivo de esta sección, ni tampoco del libro, hacer un compendio de tutoriales sobre cómo emplear las herramientas disponibles para descubrir o explotar vulnerabilidades. Estamos convencidos de que es mucho más útil exponer aspectos conceptuales y

de desarrollo de los distintos sistemas, los cuales luego son aprovechados por estas herramientas. Un ejemplo de esto podremos verlo claramente cuando hagamos mención al sistema de seguridad **WPA**, donde el principio utilizado para desarrollar un antiguo ataque contra el protocolo **WEP** (**ataque korek**) es adaptado para WPA.

Sin un conocimiento sólido, sería muy complicado siquiera detectar la posibilidad de adaptar dicho método. Si bien es cierto que la seguridad tiene un gran porcentaje de práctica y trabajo de campo, con una base conceptual sólida, podemos recurrir a la infinidad de tutoriales que existen en Internet y no solo ejecutarlos paso a paso, sino que además comprenderemos qué estamos haciendo en cada instancia.

Por eso, nos gustaría compartir una frase de Leonardo Da Vinci: "Los que se enamoran de la práctica sin la teoría son como los pilotos sin timón ni brújula, que nunca podrán saber hacia dónde van".

HISTORIA DE LAS REDES INALÁMBRICAS

Si viajamos en el tiempo, encontraremos que varias civilizaciones usaron distintos medios para enviar información entre puntos distantes de forma rápida. Ejemplos de esto podrían ser las señales de humo, las torres con antorchas que se encendían como signo de alarma, y más cercano a nuestros tiempos, el uso de palomas mensajeras.

En el siglo XIX, el físico escocés James Clerk Maxwell relacionó las ondas magnéticas con las ondas eléctricas y describió por completo los fenómenos electromagnéticos. Anteriormente a Maxwell, varios científicos de la talla de Michael Faraday, Carl Friedrich Gauss, Hans Christian Oersted, Charles de Coulomb, André Ampère y muchos más habían estudiado en forma aislada los campos eléctricos y magnéticos, pero hasta ese momento no los habían relacionado.

La genialidad de Maxwell fue desarrollar una serie de ecuaciones (posteriormente simplificadas) que relacionaban dichos campos, dando lugar a los **campos electromagnéticos**. Estas ecuaciones son conocidas como las **ecuaciones de Maxwell**. Un caso particular de estas ondas son las **radiofrecuencias**, ya que poseen ciertas características que las hacen aptas para transmitir información a través del aire. Particularmente, éstas son las que se utilizarán en las comunicaciones que nos interesan en esta sección.

Dentro de las telecomunicaciones, debemos mencionar la importancia que hoy en día tienen las redes inalámbricas

Las tecnologías de transmisiones inalámbricas se pueden clasificar, básicamente, según dos criterios: por su **alcance** y por el tipo de **acceso**. En este último caso, nos centraremos directamente en la tecnología WiFi.

Según el alcance, podemos clasificar las redes en **WPAN** (*Wireless Personal Area Network*), **WLAN** (*Wireless Local Area Network*), **WMAN** (*Wireless Metropolitan Area Network*) y **WWAN** (*Wireless Wide Area Network*).

El alcance de las WPAN está limitado hasta los 10 metros en promedio. En términos generales, se utilizan para interconectar dispositivos tales como impresoras, teclados y gadgets varios. Ejemplos de este tipo de red son las tecnologías **IrDA** y **Bluetooth**. En el caso de las WLAN, las redes que comúnmente todos conocemos, tienen un alcance máximo teórico de 300 metros aproximadamente. El estándar es el **IEEE 802.11** (**www.ieee802.org/11**), también conocido como WiFi.

Las WMAN están orientadas a brindar una red a grandes comunidades, por ejemplo, una ciudad. Un ejemplo de esta tecnología es **WiMAX**, actualmente con un alcance máximo de 70 kilómetros. El estándar de WiMAX es el **IEEE 802.16**.

Finalmente, las WWAN son las redes de mayor alcance, aquéllas que suelen cubrir grandes extensiones territoriales. Un ejemplo son las redes de datos de telefonía celular, implementadas según diversos protocolos como **GPRS**, **EDGE** y **3G** (**GSM** tercera generación).

La otra clasificación gira en función del tipo de acceso. En este caso, nos centraremos en el estándar **802.11**. Así, tendremos redes en modo **Ad-Hoc**, en modo **infraestructura** y según **múltiples puntos de acceso** (**Figura 9**).

Las redes ad-hoc se establecen cuando dos equipos directamente se conectan entre sí. Mientras ambos estén dentro del área de cobertura de la red, el funcionamiento es independiente, y cada equipo tendrá acceso a los recursos compartidos por el otro equipo, pero nunca con equipos o servidores externos a ese enlace. Comúnmente, estas redes no requieren de ningún tipo de configuración ni administración.

Es el estándar de comunicaciones desarrollado por el IEEE (Institute of Electrical and Electronics Engineers) en 1997, también conocido como WiFi

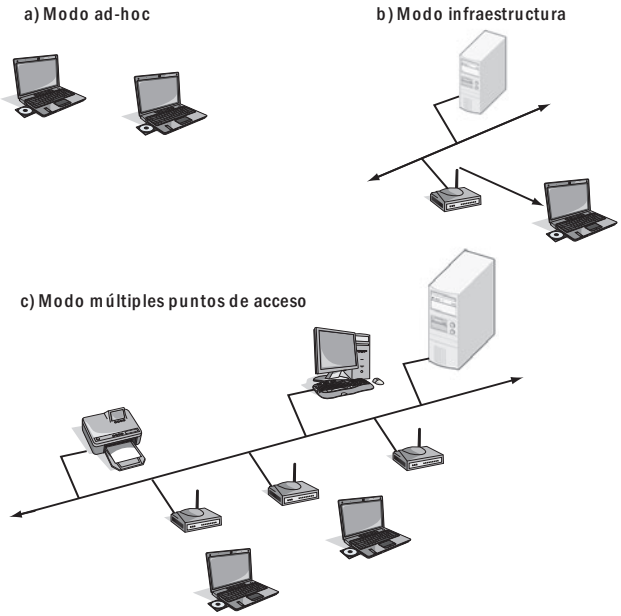


FIGURA 9. Según el modo de acceso, la red puede ser: a) modo ad-hoc, b) modo infraestructura o c) modo múltiples puntos de acceso.

En las redes en modo infraestructura, se emplea un **access point** o punto de acceso para centralizar la conexión de varios equipos. A su vez, mediante un cable enchufado a la red cableada, permite que los equipos conectados a él puedan acceder a los recursos habilitados en la red. Estos dispositivos también aumentan el rango de comunicación, ya que actúan como repetidores.

Las redes se conocen mediante un identificador denominado genéricamente **SSID**, el cual es una cadena de 1 a 32 caracteres del código ASCII, sensible a mayúsculas y minúsculas, que permite a los equipos clientes asociarse a determinada red.

Finalmente, en el caso de las redes de múltiples puntos de acceso, se utilizan varios access point distribuidos en una zona específica, con el objetivo de ampliar el rango de comunicación que brindaría un solo dispositivo. También implementan el concepto de **roaming** y permiten a los equipos cliente moverse libremente dentro de la red.

ESTÁNDAR IEEE 802.11

Es el estándar de comunicaciones desarrollado por el **IEEE** (*Institute of Electrical and Electronics Engineers*) en 1997, también conocido como WiFi. En términos más específicos, define el uso de las dos capas inferiores del modelo OSI (capa física y capa de enlace). Para la transmisión en 802.11 se utilizan catorce canales distintos, cada uno de los cuales tiene un ancho de banda de 22 MHz.

Pero la cantidad de canales útiles depende de la reglamentación de cada país. En Argentina, la Comisión Nacional de Comunicaciones (CNC) es el ente encargado de reglamentar estos y otros temas relacionados con las telecomunicaciones, como por ejemplo, licencias de RF, máximas potencias de transmisión, etcétera.

La versión original del año 1997 fue la actualmente denominada 802.11 legacy, ya obsoleta. Trabajaba a una frecuencia de 2.4 GHz y con un ancho de banda de 2 Mbps (mega bits por segundo) teóricos. En el año 1999, se publicó la primera revisión de la norma, la 802.11a, aunque los equipos recién estuvieron disponibles en 2001. Trabajaba en 5.8 Ghz y tenía un ancho de banda de 54 Mbps.

También en 1999 se publicó la modificación 802.11b, la cual ofrecía un ancho de banda de 11 Mbps máximo y trabajaba a 2.4 Ghz. En 2003, y manteniendo compatibilidad con la 802.11b, se ratificó la 802.11g, que mantenía la frecuencia en 2.4 Ghz, pero aumentaba el ancho de banda a 54 Mbps. Dada la retrocompatibilidad de esta norma con la **b**, obtuvo gran penetración en el mercado y aún hoy sigue siendo la más utilizada.

Una norma que está comenzando a extenderse en estos días es la 802.11n, también denominada **Next Generation Wi-Fi**. Si bien no está oficialmente estandarizada, ya hay varios equipos disponibles en el mercado. Busca mantener compatibilidad con 802.11a/b/g y alcanzar un ancho de banda cercano a los 600 Mbps. Para esto implementaría la tecnología **MIMO** (*Multiple Input Multiple Output*), a partir del uso de varios canales simultáneos con hasta tres antenas por equipo.

Como mencionamos, algunas normas agregaban funcionalidades al estándar; una de ellas es la 802.11i, cuyo objetivo es mejorar el nivel de seguridad para protocolos de autenticación y codificación. Esta norma abarca los protocolos 802.1x y AES.

SEGURIDAD ASOCIADA A LAS REDES INALÁMBRICAS

Desde el punto de vista de la seguridad, analizaremos algunos aspectos relacionados tanto a la configuración de las redes como a la tecnología. En el primer caso, la seguridad estará asociada a la configuración de los distintos componentes de las redes WiFi. En cuanto al aspecto tecnológico, veremos algunas particularidades que dependen de características intrínsecas de la seguridad, especialmente los mecanismos y protocolos de autenticación que fueron avanzando con el correr del tiempo.

Aspectos relacionados a la configuración de las redes

Respecto de la configuración, en primer lugar tenemos en cuenta al SSID, el identificador que ya mencionamos anteriormente. Éste es enviado por broadcast y permite que los equipos cliente lo detecten y se conecten a la red. Una opción interesante que suelen permitir la mayoría de los access point es la de deshabilitar este broadcast.

Si bien esto no brinda seguridad por el solo hecho de no habilitarlo, si se tiene en cuenta el modelo de seguridad por capas, estamos agregando una complicación más para el atacante. Un cliente válido en esta situación deberá conocer el identificador y solicitarle al punto de acceso la conexión.

Desde la perspectiva del atacante, aunque es una complicación no conocer el SSID, solo basta con *sniffear* las redes inalámbricas de la zona y esperar a que algún cliente válido se quiera conectar a la red. Este cliente en algún momento enviará el SSID y podrá ser captado por el posible atacante.

Otra etapa que también puede configurarse es la de asociación y autenticación. Una vez que ambas partes conocen el identificador, comienza el proceso de asociación. Los dos métodos que define el estándar 802.11 para que los clientes se conecten a un access point son:

WIFI ALLIANCE

A partir de la masificación de la tecnología WiFi, y para normalizar los equipos que implementan esta tecnología, se creó la **WiFi Alliance** (**www.wi-fi.org**). De esta forma, se buscaba lograr compatibilidad entre los equipos, independientemente del fabricante.

- Autenticación abierta.
- Autenticación de clave compartida (**PSK**).

Para asociarse, un cliente escucha pasivamente esperando a que el punto de acceso envíe unos paquetes de control denominados **beacon frames**. Éstos contienen datos, como ser el SSID, que permitirán al cliente obtener información del dispositivo y así poder conectarse. En el caso de la autenticación abierta, el proceso se realiza en texto plano, no se verifica ni usuario ni host.

La autenticación por clave compartida funciona de manera similar a la abierta, solo que comprueba el cliente, lo que requiere que ambos extremos tengan la misma clave compartida. Estos mecanismos originalmente estaban asociados al protocolo WEP, el primero que brindaba seguridad a las redes inalámbricas.

Complementario a estos métodos, aunque no forma parte de las especificaciones del 802.11, también puede autenticarse a través de direcciones MAC. Esto se realiza mediante una lista de control de acceso que puede estar en el dispositivo, o bien validarse frente a un servidor externo. En esta lista se agregan las direcciones MAC válidas.

Aspectos relacionados con los protocolos de seguridad

Dado que las redes inalámbricas son esencialmente inseguras, ya que cualquier usuario que disponga del equipo indicado puede conectarse a ellas, fue necesario desarrollar mecanismos tecnológicos que brinden seguridad. Para esto se fueron creando distintos protocolos y sistemas. Como ya mencionamos, el primero de ellos fue WEP.

WEP (*Wired Equivalent Privacy*) fue desarrollado en 1999 como parte del estándar IEEE 802.11. En un principio, este sistema implementaba una clave de 40 bits basada en el algoritmo **RC4** (*Rivest Cipher 4*), al cual se le descubrieron serias vulnerabilidades posteriormente. Entre las características más importantes de WEP, podemos mencionar que los mensajes se cifran junto con un **chequeo de redundancia cíclica** (**CRC**) de 32 bits y brindando integridad al sistema.

La confidencialidad está dada por el cifrado con RC4. En este caso, pueden utilizarse dos alternativas: claves de 40 bits (incrementadas a 64 bits por medio de un vector de inicialización de 24 bits) o de 104 bits (incrementadas a 128 bits por acción

WEP (Wired Equivalent Privacy) fue desarrollado en 1999 como parte del estándar IEEE 802.11

de dicho vector). La implementación de este sistema es sencilla, solo hace falta compartir la clave entre los equipos clientes y el punto de acceso. Ésta es una de las características que más propulsó el uso de este sistema.

En la actualidad, WEP no brinda ningún tipo de seguridad, ya que posee serias debilidades en distintas partes de la implementación. Debido a su fracaso, fue forzoso desarrollar un nuevo sistema que ofreciera seguridad a las redes inalámbricas. Por cuestiones de retrocompatibilidad y de urgencia en cuanto a la necesidad imperiosa de tener un buen sistema de seguridad, la **Wi-Fi Alliance** desarrolló el sistema **WPA** (*WiFi Protected Access*).

Dado que ya existía gran cantidad de equipos que implementaban WEP, no podía desarrollarse directamente un nuevo sistema que dejara obsoleto a su antecesor y obligara a los usuarios, particulares o empresas, a migrar todos sus equipos para que soportaran el nuevo estándar. Por otro lado, la premura para implementar una nueva solución no ofrecía el tiempo suficiente como para desarrollar desde cero un nuevo sistema que brindara seguridad real a las redes inalámbricas. Frente a este panorama, se creó el sistema WPA, que cubrió la brecha que dejaba WEP, pero mantuvo la compatibilidad con esos equipos, simplemente con el reemplazo del **firmware** por uno más moderno.

Mientras tanto, el IEEE comenzaba con el desarrollo de un nuevo sistema original, el cual iba a implementar los últimos avances de seguridad hasta ese momento. Así daba inicio el desarrollo de 802.11i, que comentaremos en breve.

Respecto de las mejoras que incorpora WPA sobre WEP, si bien mantiene RC4 como algoritmo, introdujo algunas características extra para fortalecer el proceso de cifrado. Por un lado, aumentó el tamaño de las claves dinámicas de 64 a 128 bits. Relacionado con esto, también duplicó el tamaño de los vectores de inicialización, de 24 a 48 bits.

Como resultado, elevó el espacio de claves a 2^{48} y redujo drásticamente la reutilización de vectores que existía en WEP. Pero el avance más importante fue la posibilidad de autenticarse contra un servidor externo en lugar de las claves compartidas de WEP. Para esto se utiliza **`TKIP`** (*Temporal Key Integrity Protocol*), un protocolo de autenticación que usa las claves dinámicamente a medida, que se utiliza el sistema. Para entornos pequeños además permite usar el método **PSK**. Otro cambio significativo estaba relacionado con la incorporación de identidad, la cual se mejoró incorporando, en lugar

del CRC, de un nuevo método de chequeo denominado **MIC** (*Message Integrity Code*), también conocido como **Michael**. Este procedimiento no tiene los problemas de linealidad que poseía el CRC y es más consistente para comprobaciones de integridad desde el punto de vista de la seguridad.

Todo esto hace que el único ataque posible contra este sistema (como así también para WPA2) sea el de fuerza bruta y el de la versión de clave compartida (al menos hasta ahora). Para ello se puede utilizar la herramienta **aircrack-ng** y una buena lista de claves prehasheadas.

Es importante recalcar que estas claves se crearon teniendo en cuenta los identificadores de redes más comunes y aquéllos que suelen venir en forma predeterminada en los distintos dispositivos. Esto es así ya que dichas tablas no solo dependen de la clave, sino también del SSID de la red. De esto último se desprendería que para tener una buena protección en la red inalámbrica, incluso en la versión PSK, es suficiente con utilizar claves fuertes y modificar los nombres de red que vienen configurados por los distintos fabricantes.

Sin embargo, durante octubre de 2008, la compañía de seguridad rusa **ElcomSoft** descubrió una

vulnerabilidad en el protocolo TKIP. El método encontrado no permite recuperar la contraseña (por lo menos todavía). Aunque el problema se haya en el cifrado, está limitado a descifrar paquetes concretos o a inyectar nuevos y en pequeñas cantidades. A partir de esto, un ataque posible sería generar una denegación de servicio o inyectar paquetes que permitan redirigir el tráfico.

Como mencionamos anteriormente, hasta ahora las agresiones implementadas permitían, a través de un ataque de fuerza bruta (usualmente con la herramienta aircrack-ng), conseguir la clave bastante rápidamente. Es importante recalcar que un ataque de fuerza bruta no supone una debilidad del WPA en sí, ya que en última instancia cualquier sistema es susceptible de ser vulnerado por fuerza bruta.

EAP

El *Extensible Authentication Protocol* (**EAP**) es un protocolo de autenticación que provee soporte para distintos tipos de comprobación en función de diferentes necesidades. Los más comúnmente utilizados son **EAP-TLS** (EAP con TLS) y **EAP-RADIUS** (EAP con RADIUS).

Es importante recordar que un ataque basado en una técnica similar a la recientemente descubierta (conocida como **Korek**) volvió obsoleto al WEP. Ésta permitía que se pudiera descifrar un paquete de tipo ARP en menos de 15 minutos, independientemente de la contraseña usada. Los analistas han observado que aprovechándose de estas similitudes, y eludiendo las mejoras introducidas con TKIP, se puede realizar un ataque de características muy parecidas al que se creó contra WEP, pero con resultados limitados. Posiblemente en un futuro no muy lejano se mejore este método y se desarrollen herramientas que lo pongan en funcionamiento (en el caso de aircrack-ng ya hay avances en torno de esta necesidad).

Paralelamente al desarrollo e implementación de WPA, el IEEE formó un grupo de trabajo para encontrar una solución definitiva al problema de la seguridad de las redes inalámbricas. En 2004 fue aprobada la edición final de este estándar, denominado 802.11i. La Wi-Fi Alliance se basó completamente en esta norma para desarrollar **WPA2**. De manera análoga a WPA, llamó a la versión de clave compartida **`WPA2-Personal`**, mientras que a la versión con autenticación 802.1x la denominó **`WPA2-Enterprise`**.

Para resolver definitivamente la problemática de la autenticación, se implementó el estándar 802.1x, con **`EAP`** o RADIUS. También permite el uso de TKIP para proporcionar seguridad a dispositivos diseñados para WEP. Por otro lado, deja de utilizarse RC4 como algoritmo de cifrado para pasar finalmente al estándar AES.

El establecimiento de la conexión en WPA2 consta de cuatro fases:

1) El acuerdo sobre la política de seguridad.
2) La autenticación por medio de 802.1x (utilizando RADIUS o EAP).
3) La generación y distribución de claves.
4) El proceso por el cual se garantiza la confidencialidad e integridad de la asociación.

RESUMEN

En este capítulo, analizamos distintos aspectos de la seguridad en infraestructura de redes. Vimos en detalle las diferentes técnicas conceptuales que dan lugar a ataques más complejos. Luego, analizamos los variados dispositivos y tecnologías de seguridad.

Multiple **choice**

1 ¿Qué sistema volvió obsoleto el Korek?

a- WPE
b- WPA
c- WPA2- personal
d- WPA2-Enterprise

2 ¿Cómo se llama el analizador de protocolos más famoso?

a- PSK
b- DMZ
c- Hijacking
d- Wireshark

3 ¿Cómo se llama la aplicación utilizada para monitorear y analizar el tráfico en la red?

a- Mic
b- Kismet
c- Smurf
d- Sniffer

4 ¿En qué año fue desarrolllado WEP?

a- 1999
b- 2001
c- 2006
d- 2009

5 ¿Cómo se llamó la versión WPA2 con clave compartida?

a- EAP
b- WPA2-Personal
c- WPA2-Enterprise
d- RADIUS

6 ¿Cómo se llamó la versión WPA2 con autenticación 802.1x?

a- EAP
b- WPA2-Personal
c- WPA2-Enterprise
d- RADIUS

Respuestas: 1-a, 2-d, 3-d, 4-a, 5-b, 6-c.

Capítulo 7
Marco legal

En este capítulo, haremos una breve reseña del panorama jurídico a nivel internacional y nacional.

Marco **legal**

En este capítulo, haremos una breve reseña del panorama jurídico, en una primera instancia a nivel internacional, y luego puntualizaremos en el caso de la legislación Argentina: mencionaremos y comentaremos brevemente cuáles son las leyes relacionadas con la seguridad de la información.

Introducción

En el contexto general mencionado a lo largo del presente libro, se hace imperiosa la necesidad de contar con un marco legal propicio que regule la actividad, tanto en el aspecto internacional como en el nacional.

En el último tiempo, se ha prestado especial interés en el ámbito internacional y se ha llegado a un consenso en las valoraciones político-jurídicas de los problemas asociados al mal uso de un equipo informático, lo cual hizo que, en algunos casos, se modificaran los derechos penales nacionales e internacionales.

En particular, la **Organización de las Naciones Unidas** (ONU) señala que, cuando los problemas llegan al ámbito internacional, se amplifica su magnitud y los delitos informáticos se constituyen en una forma de crimen transnacional. Respecto a qué considera como delitos informáticos, propone la siguiente segmentación:

- **Fraudes cometidos mediante manipulación de computadoras**: dentro de esta categoría, podemos citar ataques que tengan como objetivos la manipulación de los datos de entrada, de los datos de salida, de programas o el fraude efectuado por medio del mal manejo informático.
- **Modificación de datos de entrada**: en esta categoría, podemos hacer, a su vez, dos divisiones: cuando la manipulación se realiza con el objeto de modificar datos almacenados en forma digital en

El primer caso de abuso contra una computadora se registró en Estados Unidos en el año 1958

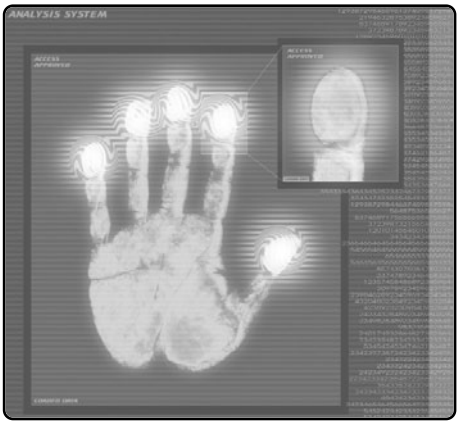
determinado equipo, o bien cuando se manipulan datos para falsificar documentos de uso comercial.

- **Daños o modificaciones de programas o datos digitalizados**: en esta categoría, contemplamos el sabotaje informático, el acceso no autorizado a servicios y sistemas informáticos, y la reproducción no permitida de programas informáticos de protección legal, entre otros.

Además de los tipos de delitos reconocidos por la ONU, el **XV Congreso Internacional de Derecho**, realizado en la ciudad brasileña de Río de Janeiro en el año 1994, ha propuesto todas las formas de conductas lesivas de la que puede ser objeto la información. Éstas son: fraude en el campo de la informática, falsificación en materia informática, sabotaje y daños a datos computarizados o software, acceso no autorizado, intercepción de información sin autorización, reproducción no autorizada de un programa informático protegido, espionaje informático, uso no autorizado de una computadora, tráfico de claves informáticas obtenidas por medio ilícito y distribución de virus o programas delictivos.

UN POCO DE HISTORIA INTERNACIONAL

El primer caso de abuso contra una computadora se registró en Estados Unidos en 1958, pero no fue hasta 1966 que se llevó adelante el primer proceso judicial por la alteración de datos de un banco de Minneapolis. Durante la primera parte de la década del 70, mientras especialistas y criminólogos discutían si el delito informático era el resultado de una nueva tecnología, los ataques de este tipo se hicieron más frecuentes. Con el objetivo de acelerar las comunicaciones, enlazar compañías, centros de



investigación y transmitir datos, las redes tenían que (y todavía tienen) ser accesibles desde varios puntos. Debido a esto, el Pentágono, la OTAN, las universidades, la NASA, y los laboratorios industriales y militares se convirtieron en el blanco primario de los atacantes.

Pero hubo dos hechos que marcaron un punto de inflexión desde el lugar del procedimiento policial frente a este tipo de casos. En 1976, por un lado, el FBI dictó un curso de entrenamiento para sus agentes acerca de delitos informáticos. Por otro lado, en forma paralela, el **Comité de Asuntos del Gobierno de la Cámara** de Estados Unidos presentó dos informes que dieron lugar a la ley federal de **Protección de Sistemas** de 1985.

Esta norma fue la base para que los estados de Florida, Michigan, Colorado, Rhode Island y Arizona se constituyeran en los primeros en contar con legislación específica, anticipándose un año al dictado de la *Computer Fraud and Abuse Act* de 1986.

Ésta se refería, en su mayor parte, a delitos de abuso o de fraude contra casas financieras, registros médicos, computadoras de instituciones financieras o involucradas en delitos interestatales. También especificaba penas para el tráfico de claves con la intención de cometer fraude y declaraba ilegal el uso de contraseñas ajenas o propias en forma inadecuada.

Un año después, se adoptó el **Acta Federal de Abuso Computacional** (18 USC Sec 1030), que modificó la de 1986 (**Figura 1**). Esta actualización tiene en cuenta la regulación de los virus, aunque no los limita al malware existente, sino que contempla y extiende el concepto a las variantes que pueden contaminar otros grupos de programas o bases de datos.

Para la misma época, en Alemania, con el objetivo de hacer frente a los delitos informáticos, el 15 de mayo de 1986 se adoptó la segunda ley contra la **Criminalidad Económica**, que reformó el Código Penal alemán (artículo 148° del 22 de diciembre de 1987) para contemplar algunos de los siguientes delitos: **espionaje de datos**, **estafa informática**, **falsificación de datos probatorios**, etcétera.

También en Europa, España sea quizás el país que mayor experiencia ha obtenido en casos de este tipo de delitos. Su actual ley orgánica de **Protección de Datos de Carácter Personal** fue aprobada el 15 de diciembre de 1999. Reemplaza una veintena de leyes anteriores de la misma índole y contempla la mayor cantidad de acciones lesivas sobre la información. Sanciona en forma detallada la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, el hacking malicioso o militar, el phreaking, la contaminación con virus, etcétera. Prevé las penas de prisión y de multa, y las agrava cuando existe una intención dolosa o cuando el hecho es cometido por parte de funcionarios públicos.

Su nuevo código penal establece castigos de prisión y multas a "quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos,

FIGURA 1.
En Internet, podemos leer el texto original del 18 United State Code Sección 1030.

programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".

En Latinoamérica, Chile fue el primer país en sancionar una ley que castigue los delitos informáticos. El 7 de junio de 1993 se publicó en el Diario Oficial la Ley 19.223, que tipifica figuras penales relativas a la informática y señala que la destrucción o la inutilización de un sistema de tratamiento de información puede ser castigado con prisión.

EL PANORAMA ARGENTINO

Desde el punto de vista argentino, podemos analizar dos aproximaciones. Por un lado, con relación a los tratados internacionales que tienen rango constitucional, a partir del artículo 75° inciso 22 de la **Constitución Nacional** reformada en 1994.

Por otro lado, tenemos las leyes sancionadas en la Argentina, que contemplan la seguridad de la información y los delitos informáticos.

Adicionalmente a la perspectiva de la ONU, que sostiene que una forma de resolver los problemas que involucran a varios países es recurrir a los tratados internacionales a los cuales adhirió la Argentina, el país también es parte del acuerdo que se celebró en el marco de la **Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio**, que en su artículo 10° relativo al software y compilaciones de datos establece:

- Este tipo de programas, ya sean tanto código fuente como objeto, serán protegidos como obras literarias en conformidad con el **Convenio de Berna**, de julio del año 1971, para la **Protección de Obras Literarias y Artísticas**.
- Las compilaciones de datos legibles serán protegidas como creaciones de carácter intelectual.
- Para los casos de falsificación dolosa de marcas de fábrica y de comercio o de **piratería lesiva del derecho de autor a escala comercial**, se establecerán procedimientos y sanciones penales

además de que los recursos disponibles comprenderán la prisión y/o la imposición de penas pecuniarias suficientemente disuasorias.

También fueron suscritos otros convenios tales como la convención sobre la **Propiedad Intelectual de Estocolmo** (julio de 1967) el 17 de marzo de 1980 por la Ley 22.195 y el Convenio de Berna, el 8 de julio de 1990.

Paralelamente a los casos anteriores, fueron ratificadas la **Convención para la Protección y Producción de Fonogramas** de octubre de 1971 por la Ley 19.963 del 23 de noviembre 1972 y la **Convención Relativa a la Distribución de Programas y Señales** de abril de 1994 por la Ley 24.425 del 23 de diciembre de 1994.
Existen otros **convenios no ratificados** aún por la Argentina, realizados por la **OMPI** (Organización Mundial de la Propiedad Intelectual), de la que el país es parte integrante a partir del 8 de octubre de 1980.

A partir de estos tratados y de la experiencia obtenida por otros países en materia de legislación de seguridad de la información, en particular de delitos informáticos, la Argentina cuenta con una serie de leyes asociadas a dicha temática. En particular, las leyes 11.723 y 25.036 relacionadas con la **Propiedad**

Intelectual, la Ley 24.766 de **Confidencialidad**, la Ley 25.326 de **Protección de Datos Personales** (**hábeas data**), la Ley 25.506 de **Firma Digital** y, finalmente, la Ley 26.388 de **Delitos Informáticos**.

La Ley de Confidencialidad sancionada en febrero de 1997 protege la información confidencial a través de acciones penales y civiles, y considera que es aquélla que cumple los siguientes puntos:

- Es secreta en el sentido de que no sea generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza este tipo de información.
- Tiene valor comercial por el hecho de ser secreta.
- Existen medidas para mantenerla secreta, tomadas por la persona que legítimamente la controla.

BIBLIOGRAFÍA Y REFERENCIAS

Artículos de SeguInfo: **www.segu-info.com.ar/delitos**, Ley de Propiedad Intelectual (modificatoria): **www.mincyt.gov.ar/25036.htm**, Ley de Confidencialidad: **www.mincyt.gov.ar/2476696.htm** y Ley de Protección de Datos Personales: **http://infoleg.mecon.gov.ar**.

Por medio de esta ley, la sustracción de distintos medios de almacenamiento y el acceso sin autorización a una red o a una computadora que contenga información confidencial serán sancionados con la pena de violación de secretos. Luego de varios años de espera, finalmente, el 4 de junio de 2008 se convirtió en ley (26.388) el **Proyecto de Delitos Informáticos** con 172 votos a favor y ninguno en contra. Esta norma modifica el **Código Penal** argentino para incluir los delitos informáticos y sus respectivas penas (**Figura 2**). A partir de su sanción, el Código Penal contempla los siguientes tipos de delitos:

- Distribución y tenencia de pornografía infantil con fines de distribución.
- Violación de correo electrónico.
- Acceso ilegítimo a sistemas informáticos.
- Daño informático y distribución de virus.
- Daño informático agravado.
- Interrupción de comunicaciones.

Esta ley no regula el spam, que ya era considerado ilegal bajo el artículo 27° de la Ley 25.326 de **Protección de Datos Personales**, pero un envío masivo de correos que obstruya y, por ejemplo, genere una denegación de servicio a un sistema informático podría considerarse como el delito previsto en el artículo 197° (**interrupción de comunicaciones**).

Es necesario recalcar que esta ley y las modificaciones asociadas al Código Penal generan mucha controversia en algunos puntos, pero lo cierto es que establecen las bases legales para comenzar a actuar en casos en donde hasta este momento era imposible incursionar.

BOLETIN OFICIAL
DE LA REPUBLICA ARGENTINA

Buenos Aires, miércoles 25 de junio de 2008
Año CXVI
Número 31.433
Precio $ 0,80

Primera Sección
Legislación y Avisos Oficiales

Sumario

Pág.

LEYES

CODIGO PENAL
26.388
Modificación. 1

PARQUES NACIONALES
26.389
Modificación de la Ley Nº 22.351. 3

PROHIBICION DEL TRABAJO INFANTIL Y PROTECCION DEL TRABAJO ADOLESCENTE

LEYES

CODIGO PENAL

Ley 26.388

Modificación.

Sancionada: Junio 4 de 2008
Promulgada de Hecho: Junio 24 de 2008

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de

FIGURA 2.
Un extracto del Boletín Oficial de la Argentina del día miércoles 25 de junio de 2008, donde aparece publicada la Ley de delitos informáticos (26.388).

RESUMEN

En este último capítulo, conocimos todo sobre la legislación internacional y nacional relacionada con los delitos informáticos. Relizamos un marco histórico de su desarrollo hasta las últimas actualizaciones en la normativa argentina.

Multiple **choice**

1 ¿En qué año se llevó adelante el primer proceso judicial por la alteración de datos?

a- 1958
b- 1966
c- 1978
d- 1996

2 ¿En qué año se registró el primer caso de abuso contra una computadora?

a- 1958
b- 1966
c- 1978
d- 1996

3 ¿En qué ley Argentina se encuentra regulado el spam?

a- 25.326
b- 11.723
c- 26.388
d- 24.425

4 ¿En qué ley se encuentra regulada la distribución de virus informáticos?

a- 25.326
b- 11.723
c- 26.388
d- 24.425

5 ¿En qué ley se encuentra regulado el uso de la firma digital?

a- 25.326
b- 11.723
c- 26.388
d- 25.506

6 ¿En qué ley se encuentra regulada la protección de datos personales?

a- 25.326
b- 11.723
c- 26.388
d- 25.506

Respuestas: 1-b, 2-a, 3-a, 4-c, 5-d, 6-a.

Capítulo 8

Penetration Testing

En este capítulo, nos centraremos en el Penetration Testing y veremos sus distintas fases.

Penetration **Testing**

En este capítulo, comenzaremos por definir algunos conceptos clave de la seguridad informática y analizaremos, brevemente, distintos tipos de análisis de seguridad. Luego, nos centraremos en el Penetration Testing y veremos sus distintas fases: reconocimiento, escaneo, enumeración, acceso y, finalmente, mantenimiento del acceso.

Introducción

En esta primera sección, repasaremos algunos conceptos para ponernos de acuerdo con la terminología. Algunos de ellos son los de la tríada **CIA** (**Confidencialidad**, **Integridad**, **Disponibilidad**), relacionados con la **identificación**, **autenticación** y **autorización**, entre otros aspectos (**Figura 1**). Luego, haremos una breve recorrida por los distintos tipos de controles que pueden ser implementados y, para concluir, veremos algunos de los tipos de análisis que se pueden realizar.

DEFINICIONES Y CONCEPTOS GENERALES

Mucho se ha escrito ya sobre conceptos de seguridad informática, sobre la **tríada CIA** y otros términos asociados, por lo que no profundizaremos demasiado en ellos, pero sí los refrescaremos brevemente.

En primer lugar, definiremos esa frase tan conocida que solemos repetir continuamente y que tanto misterio despierta: **seguridad informática**. Con más o menos palabras, se la define como *el conjunto de*

La integridad nos indica que toda modificación de la información solo es realizada por usuarios autorizados, por medio de procesos autorizados

CONCEPTOS ASOCIADOS A LA TRÍADA

Identificación: mecanismo por el cual los usuarios comunican su identidad a un sistema. **Autenticación:** comprueba que la información de identificación corresponda al sujeto que la presenta. **Autorización:** corresponde a los derechos y permisos otorgados a un usuario.

medidas preventivas, de detección y corrección destinadas a proteger la integridad, la confidencialidad y la disponibilidad de los recursos informáticos. En términos generales, todos coincidiremos con ello y si partimos de la segunda parte de esta definición, nos encontramos con los tres pilares de la seguridad informática: **integridad**, **confidencialidad** y **disponibilidad**, también conocidos por sus siglas en inglés como la tríada **CIA** (*Confidentiality, Integrity, Availability*, en español Confidencialidad, Integridad y Disponibilidad).

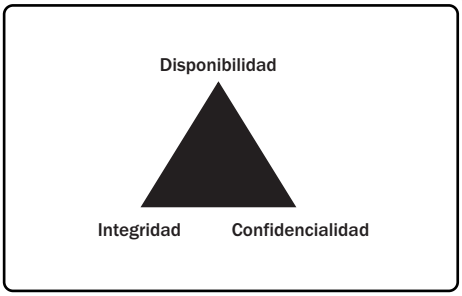


FIGURA 1. Tríada CIA (Confidencialidad, Integridad y Disponibilidad).

Para desempolvar más conceptos, definámoslos brevemente. Hablamos de **confidencialidad** cuando nos referimos a la característica que asegura que los usuarios (sean personas, procesos, etcétera) no tengan acceso a los datos a menos que estén autorizados para ello. Por otro lado, la **integridad** nos indica que toda modificación de la información solo es realizada por usuarios autorizados, por medio de procesos autorizados. La **disponibilidad** garantiza que los recursos del sistema y la información estén disponibles únicamente para usuarios autorizados en el momento que los necesiten.

Retomando la definición de seguridad informática, si nos centramos en la primera parte de la definición, debemos analizar las medidas o controles que se implementan para preservar la tríada, ya que cualquier medida de seguridad que se tome, siempre tiende a preservar uno o más de sus componentes. En la siguiente sección, las veremos en detalle.

Los **controles**

El objetivo de la seguridad informática es **fortalecer** una o varias de las características de seguridad mencionadas, mitigando de esta forma los efectos producidos por las **amenazas** y las **vulnerabilidades**. El riesgo de sufrir un incidente de seguridad nunca lo vamos a poder eliminar por completo, pero sí vamos a reducirlo a un nivel tolerable por nuestra organización.

MÁS SOBRE LA TRÍADA

Trazabilidad: habilidad para determinar las acciones individuales de un usuario dentro del sistema. **Privacidad**: nivel de confidencialidad que se brinda a un usuario. **No repudio**: utilización de elementos de información única para validar la acción de un usuario.

Estos controles pueden clasificarse según dos criterios (**Figura 2**). Por un lado, dependiendo del **momento** en el que se actúa, tendremos **controles** preventivos, disuasivos, detectivos, correctivos y recuperativos. Los **preventivos** y **disuasivos** toman acción en momentos **anteriores** al incidente, con el objetivo de evitarlo. Los **detectivos** buscan detectar el incidente en el momento en que éste está ocurriendo. Finalmente, los **correctivos** y **recuperativos** tienen lugar una vez que el incidente ocurrió.

Por otro lado, según el tipo de **recursos utilizados**, vamos a clasificarlos en controles físicos, técnicos o lógicos y administrativos. Los **controles físicos** serán aquéllos que implementen medidas de seguridad física, como por ejemplo, cerraduras electrónicas, sistemas de acceso biométrico, etcétera. Los **controles técnicos o lógicos** implementan, usualmente, medidas de carácter tecnológico, como sistemas de detección de intrusos, seguridad de las aplicaciones y sistema operativo, etcétera.

Para finalizar, son muy importantes, aunque muchas veces desvalorizados, los **controles administrativos**. La importancia de estas medidas radica en que son las que suelen determinar, en función de la política de seguridad, las configuraciones que deben cumplir el resto de los controles (**Figura 3**). Por ejemplo, las configuraciones de los controles de acceso y las reglas (desde el punto de vista de las políticas de acceso) que deben implementarse en un firewall.

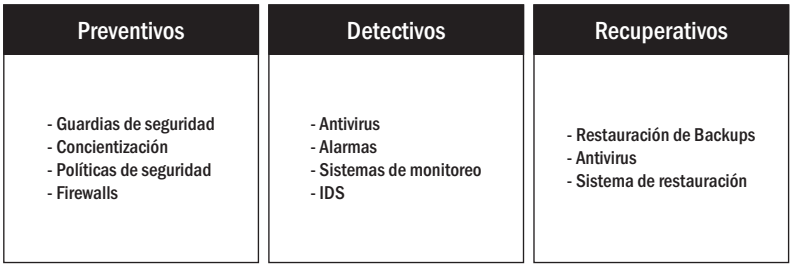


FIGURA 2. **Podemos apreciar los controles divididos en función del momento del incidente.**

MÁS INFORMACIÓN SOBRE CONTROLES

Para mayor información sobre los tipos de controles, es recomendable consultar bibliografía relacionada con la certificación **CISSP**. Por ejemplo, **CISSP All-in-One Exam Guide** (3rd Edition, Shon Harris) y **Official (ISC)2 Guide to the CISSP Exam** (Susan Hansche), entre otras.

Muchas veces, estos controles pertenecen a más de una categoría a la vez, según el punto de vista que tengamos en cuenta. Para analizar la efectividad de esos controles se realizan distintos **análisis de seguridad**. A continuación, veremos dos de ellos: **vulnerability assessment** y **ethical hacking**.

VULNERABILITY ASSESSMENT

Un **VA** (*Vulnerability Assessment)* es un análisis de **puntos débiles** o **vulnerabilidades** de carácter técnico realizado a un sistema, el cual no necesariamente tiene que estar relacionado con los sistemas informáticos o de telecomunicaciones. Este tipo de análisis también se aplica a diversos campos, como plantas de energía nuclear, procesos de biotecnología, sistemas de distribución de agua, sistemas de distribución de energía y un sinfín de otros ejemplos. En términos generales, estas evaluaciones buscan determinar las amenazas, agentes de amenaza y vulnerabilidades a las que está expuesto el sistema.

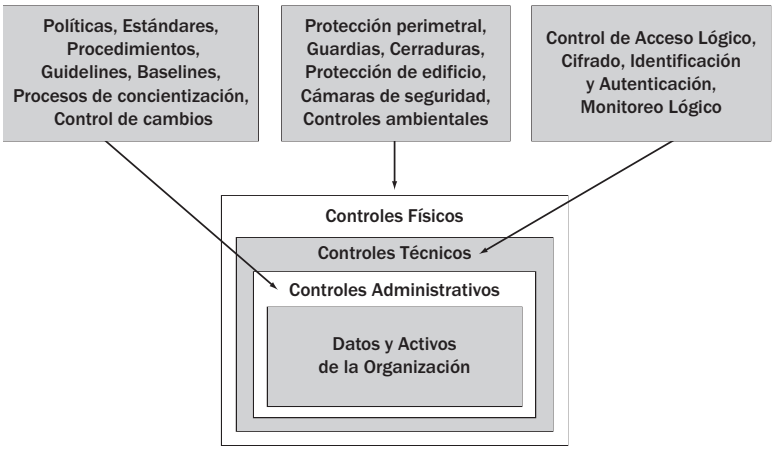


FIGURA 3. Podemos apreciar los controles en función de los recursos y ejemplos de cada uno.

EL INGENIERO SOCIAL

Este título de honor corresponde a Kevin David Mitnick, el hacker sobre quien se han escrito varias novelas y una película (**Takedown**). Dos libros de su autoría muy interesantes y de fácil lectura son **The Art of Deception** y **The Art of Intrusion**, ambos de la editorial Wiley & Sons.

Esas debilidades están relacionadas con aspectos técnicos que dependen de las características y del contexto en que está implementado el sistema que es evaluado. En nuestro caso, vamos a referirnos a un VA cuando realicemos un análisis técnico de las vulnerabilidades de una infraestructura de informática y de telecomunicaciones. Puntualmente, se analizarán vulnerabilidades asociadas a distintos servidores, redes, sistemas operativos, aplicaciones, etcétera, todas ellas relacionadas a aspectos técnicos.

Fases de un **Penetration Test**

En esta sección, haremos una breve descripción del concepto de Penetration Test y luego veremos sus distintas fases. Vale la pena aclarar que la clasificación en función de las fases que presentaremos no es única, sino que está hecha sobre la base de criterios y experiencia de los autores y otros colegas.

Veremos la fase de reconocimiento, donde analizaremos distintas técnicas y métodos

En primera instancia, veremos la fase de **reconocimiento**, donde analizaremos distintas técnicas y métodos. Luego, la fase de **escaneo**, en la cual relevaremos información relativa a la infraestructura, y algo análogo haremos en la fase de **enumeración**. En la fase de **acceso**, utilizaremos los medios necesarios para ingresar al sistema objetivo y, finalmente, en la etapa de **mantenimiento**, tomaremos las medidas necesarias para poder acceder al sistema cada vez que lo necesitemos.

FASE DE RECONOCIMIENTO

Antes de comenzar con el análisis de esta etapa, repasemos brevemente algunas características de un **pentest**. En primera instancia, podremos categorizarlo en función de los datos disponibles y los alcances de

TEXTOS SAGRADOS

Toda biblioteca digital hacker debería contar con los siguientes recursos: **Hacker Crackdown** (Bruce Sterling, 1992), **Hackers, Heroes of The Computer Revolution** (Steven Levy, 1996), **¿Cómo llegar a ser hacker?** (Eric S. Raymond) y **La catedral y el bazar** (Eric S. Raymond).

la evaluación. Así, tendremos los análisis tipo **White box** y **Black box**. En el primero de los casos, el tester tiene a su disposición información sobre la infraestructura de la empresa y la profundidad del análisis está pactada de antemano.

En el segundo, no se dispone prácticamente de información del objetivo, con lo cual en este caso la fase de reconocimiento es fundamental. El analista llegará hasta donde sus habilidades y las medidas de seguridad implementadas se lo permitan. En la práctica, la mayoría de estos tests suelen ser **híbridos**, por lo que encararemos el análisis de estas fases teniendo este punto en mente. Ahora sí, sin más preámbulos, comencemos a ver las características de la fase de reconocimiento.

Esta fase es la que más tiempo insume dentro de la planificación. Lo que se busca en primera instancia es **definir** al objetivo y, a partir de ello, obtener la mayor cantidad de información sobre él. Para el caso de **personas físicas**, ejemplos de recopilación de información serían direcciones de e-mail, direcciones físicas, información personal, etcétera. En el ámbito corporativo, además se buscarán direcciones IP, resolución de nombres DNS, etcétera. En esta parte, denominada **gathering information**, el atacante utiliza varias técnicas o metodologías, por ejemplo, el **footprinting**, la **ingeniería social** y el **dumpster diving** (*trashing*).

La importancia de esta fase radica en la necesidad de determinar el objetivo y obtener toda la información posible (dependiendo del alcance pactado con la organización), que permita llevar a cabo un ataque exitoso. En este sentido, la preparación es crítica ya que, al momento del ataque, no hay tiempo para detenerse y volver a empezar.

Según cómo se realice la búsqueda de información, tenemos dos métodos distintos. El primero de ellos son las **búsquedas online**, donde vamos a buscar información a través de Internet (**Figura 4**). En cambio, la **búsqueda offline** abarca técnicas como las mencionadas: dumpster diving e ingeniería social (debido a su extensión e importancia, estas técnicas tienen un capítulo completo dedicado a ellas).

Una de las técnicas más utilizadas para realizar búsquedas online es la de **Google Hacking**. Consiste

FIGURA 4.
Búsqueda de servidores web IIS corriendo sobre Windows 2000 (potencialmente vulnerables).

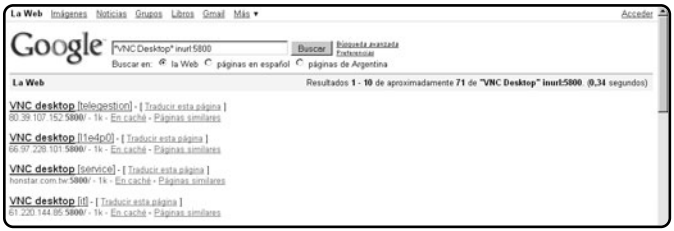


FIGURA 5.
Búsqueda de equipos que habilitan la conexión por VNC a través de HTTP.

en emplear las funciones de búsquedas avanzadas del conocido buscador, combinadas de forma tal que permitan obtener información muy precisa, como por ejemplo, equipos conectados a Internet que utilicen un sistema operativo en particular que tiene ciertas vulnerabilidades conocidas. Otro ejemplo sería, mediante ciertas cadenas de búsqueda, encontrar dispositivos específicos conectados a Internet, etcétera (**Figuras 5** y **6**).

En esta etapa, casi no se usan herramientas de software, ya que en la mayoría de los casos, con una alta dosis de paciencia y pericia en el uso de los parámetros avanzados de búsqueda de los navegadores, es posible encontrar una gran cantidad de información.

Por otro lado, para complementar esa información, existen varios sitios web con recursos online que ofrecen mucha información referente a dominios, servidores DNS y demás. Por ejemplo, **Goolag** es un recurso online (**www.goolag.org**) que podemos utilizar para buscar vulnerabilidades en dominios o

Una de las técnicas más utilizadas para realizar búsquedas online es la de Google Hacking

GOOGLE HACKING

Es un término propuesto por Johnny Long, que se refiere al uso de los parámetros de búsqueda avanzada de Google para obtener información en la fase de reconocimiento. También desarrolló el concepto de **GHDB** (*Google Hacking Data Base*).

FIGURA 6.
Búsqueda de dispositivos Cisco VPN 3000 Concentrators.

sitios de Internet, con técnicas de Google Hacking (**Figura 7**). Otro sitio, que puede resultar de gran utilidad, es **KartOO** (**www.kartoo.org**), que nos permite ver, en forma gráfica, cómo se relacionan los enlaces que posee un sitio (**Figura 8**).

Además de Google Hacking y los sitios que vimos, otra alternativa para buscar información online es el uso de ciertas extensiones para el navegador **Mozilla Firefox**. Actualmente, existe una gran cantidad de plugins que agregan funcionalidades desde la óptica del tester de seguridad informática.

Recomendamos tomarse un tiempo para recorrer el sitio de extensiones de este popular navegador. Algunas de estas extensiones son **AS Number** (**Figura 9**), que nos brinda información sobre los

FIGURA 7. Goolag es un buscador optimizado para buscar sitios vulnerables.

sistemas autónomos (podemos encontrar lo que son estos sistemas en **http://es.wikipedia.org/wiki/Sistema_autónomo**), **PassiveRecon**, que centraliza varios de los recursos online vistos para darnos información sobre un determinado sitio y

MÁS SOBRE GOOGLE HACKING

Podemos encontrar más información sobre Google Hacking en el sitio de su creador, **http://johnny.ihackstuff.com/ghdb** y también, en libros como **Google Hacking for Penetrarion Testers**, de la editorial Syngress y **Google Hacks**, de editorial O´Reilly.

FIGURA 8.
Kart00 permite relacionar en forma intuitiva los enlaces que referencia un sitio web.

HackBar, que nos permite auditar la seguridad de distintos sitios web (**Figura 10**).

FASE DE ESCANEO

En esta fase, utilizaremos la información previa con el objetivo de **detectar vectores de ataque** en la infraestructura de la organización. En primer lugar, comenzaremos con el **escaneo de puertos** y **servicios** del objetivo (**Figuras 11** y **12**). Determinamos qué puertos se encuentran abiertos, y luego, asociamos el puerto a un servicio dado. Una vez que hemos finalizado con esto, llega el turno del **escaneo de vulnerabilidades**. Éste nos permitirá encontrar vulnerabilidades en el o los equipos objetivo, tanto del sistema operativo como de las aplicaciones.

FIGURA 9. El complemento AS Number **es muy utilizado para recopilar información sobres sistemas autónomos.**

RECURSOS ONLINE

A continuación, mencionamos algunos recursos online complementarios a técnicas como la de Google Hacking: Traceroute.org (**www.traceroute.org**), Whois.Net (**www.whois.net**), Maltego (**www.paterva.com/maltego**) y FixedOrbit (**www.fixedorbit.com**).

FIGURA 10.
HackBar
es un complemento muy completo que se utiliza para realizar auditorías de sitios y aplicaciones web.

Conceptualmente, a todo este proceso lo podremos dividir en seis etapas. En cada una de ellas buscaremos distintos tipos de información, desde los equipos online en una red o segmento hasta la planificación del ataque en sí mismo. Vale la pena aclarar que esta división es conceptual, ya que las herramientas suelen cubrir varias etapas juntas en un mismo análisis. Estas etapas son: detección de sistemas vivos o activos, escaneo de puertos, detección del sistema operativo, identificación de servicios, escaneo de vulnerabilidades y planificación del ataque.

Para empezar, la forma más simple de ver si un **host** está activo es a partir de la técnica de **ping sweep**, que consiste en enviar paquetes ping por **broadcast** a los hosts de una red. Si responde, implica que está online y que es un objetivo potencial de ataque. Pero si un escaneo realizado con ping sweep no detecta hosts vivos, no significa que éstos no existan. Suele utilizarse como complemento de otras técnicas, ya que por sí sola no es muy precisa.

Como segunda etapa, el análisis a partir de los puertos abiertos es el complemento ideal para el ping sweep: si a un equipo se le pueden analizar los puertos, implica que está activo.

Sin entrar en detalles, para este análisis se pueden usar varios tipos de escaneos que aprovechan distintas características del protocolo TCP (particularmente, la combinación de sus flags y la implementación del protocolo para distintos sistemas operativos). Podemos mencionar algunos de ellos, como **SYN stealth can**, **FIN scan**, **XMAS tree scan**, **NULL scan**, **FIN scan**, etcétera.

FIREFOX Y LAS EVALUACIONES DE SEGURIDAD

Desde la aparición de Firefox, el mundo de los navegadores ya no es el mismo. Continuamente están apareciendo extensiones que agregan funcionalidades. Recomendamos ingresar en **www.security-database.com/toolswatch/turning-firefox-to-an-ethical**.

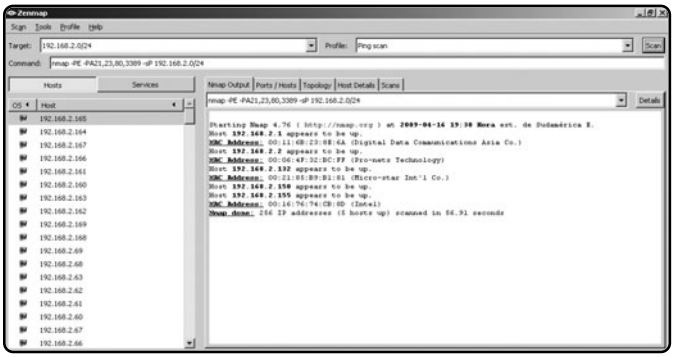


FIGURA 11.
El escáner de puertos Zenmap, versión gráfica del clásico Nmap, realizando una detección de sistemas vivos mediante el ping scanner.

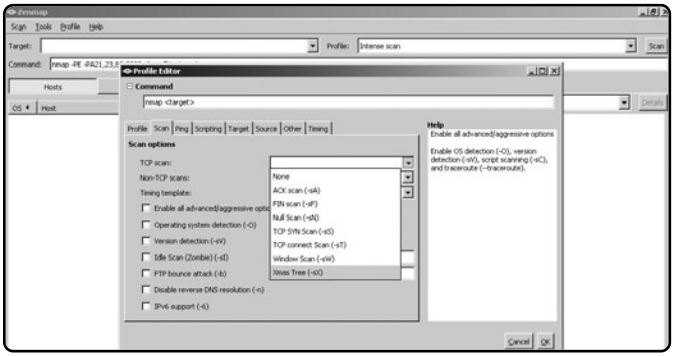


FIGURA 12.
En Zenmap podemos generar y definir un perfil de escaneo en función de nuestras necesidades.

La tercera fase, la de detección del sistema operativo, se realiza a partir de las respuestas que el host brinda frente a determinados paquetes. Cada sistema operativo tiene su implementación del protocolo TCP, y responde de manera diferente a ciertos paquetes que son interpretados por la aplicación una vez recibidos.

LOS FLAGS TCP EN EL ESCANEO DE PUERTOS

Los seis flags de TCP relacionados con los escaneos son: **SYN**, **ACK**, **PSH**, **URG**, **FIN** y **RST**. Para obtener más datos, podemos visitar el siguiente enlace: **http://sun-microsystems.org/Tecnicas_de_Deteccion/x215.html**, donde encontraremos información en español.

El análisis a partir de los puertos abiertos es el complemento ideal para el ping sweep

Como cuarta etapa, tenemos la **identificación de servicios**. A grandes rasgos, esto podemos hacerlo a partir del **banner grabbing**, que implica obtener información de la aplicación con la lectura de banners predeterminados. Recordemos que los banners son leyendas que traen las aplicaciones donde se brinda información sobre ellas, como la versión, la arquitectura, etcétera. De forma más sencilla, esto también podemos hacerlo al asociar los puertos abiertos, hallados en la etapa de escaneo, con el servicio brindado en ese puerto.

Con los datos recopilados en las etapas anteriores, comenzaremos con el escaneo de vulnerabilidades. Esto es, dependiendo de los servicios que se estén brindando (web, e-mail, FTP, etcétera), del sistema operativo base del equipo (Windows, Linux, Solaris, Mac OSX, etcétera) y la aplicación (IIS, Apache, etcétera), se podrá determinar la existencia de vulnerabilidades conocidas y así poder explotarlas posteriormente. Para el caso de vulnerabilidades desconocidas, se utilizan otras técnicas.

Finalmente, la planificación del ataque tendrá como objetivo llevar a cabo el proceso de **anonimización** y **ocultación** de huellas del ataque. Como estamos en la piel del atacante, es importante que, al momento de ingresar al sistema, no queden rastros de lo que se hizo ni cómo se hizo. Esta sexta etapa tiene en cuenta diversas técnicas para llevar esto a cabo, pero escapan al alcance de este libro.

FASE DE ENUMERACIÓN

El objetivo de esta fase es obtener información relativa a los usuarios, nombres de equipos, recursos y servicios de red. Para esto, se generan **conexiones activas** con los sistemas y se realizan **consultas directas** para obtener la información. A diferencia del caso anterior, las consultas siempre se hacen al equipo objetivo y en forma activa, lo que trae aparejado que

LOS CAZADORES DE VULNERABILIDADES

Cuenta la leyenda que quienes buscan vulnerabilidades son oscuros personajes con gran conocimiento técnico. Para llevar adelante sus investigaciones, utilizan una serie de técnicas entre las que se destacan la auditoría del código fuente, fuzzing e ingeniería inversa.

las conexiones puedan ser detectadas y registradas. En las fases anteriores, un punto importante es que estas técnicas suelen llevarse a cabo en la red interna.

Con estas consideraciones, resulta evidente que la forma de encarar la enumeración de sistemas Windows Unix/Linux es distinta. Deberemos usar técnicas y herramientas diferentes, según el tipo de sistema que analicemos. No será lo mismo obtener información de usuarios de un **Active Directory**, de un **OpenLDAP** o de un servidor **NIS**. Respecto de los recursos de red y compartidos, éstos podrían enumerarse a partir del mismo protocolo **NETBIOS** o a través de **SNMP** cuando fuese posible (**Figuras 13** y **14**). Para el caso de las aplicaciones, podemos tener una primera aproximación si empleamos comandos simples como **telnet** y **netcat** (**nc**), los cuales establecen conexiones a distintos puertos y permiten obtener banners, dependiendo de la aplicación y de su configuración.

FASE DE ACCESO

Una vez detectadas las vulnerabilidades, el gran paso es el **ingreso al sistema** definido como objetivo. Si esto se realiza en el marco de una **simulación** o de un penetration test hecho por profesionales, no se suele tomar control sobre el sistema sino detectar las vulnerabilidades y proponer soluciones.

En un ataque o simulación más realista, esta fase será quizá la que produzca la mayor descarga de adrenalina, ya que aquí se utilizan los recursos y conocimientos de manera condensada.

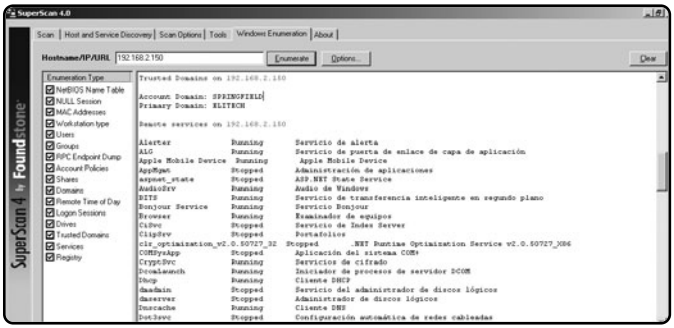


FIGURA 13.
SuperScan, de la empresa Foundstone, es un escáner de puertos, que además incluye utilidades de enumeración.

LA PIEDRA FUNDAMENTAL

Foundstone Inc. es una empresa fundada por George Kurts en 1999. En sus inicios, ofrecía herramientas de software y servicios, hasta que en 2004 fue adquirida por **McAfee**. Muchas herramientas clásicas de seguridad fueron creadas por esta compañía.

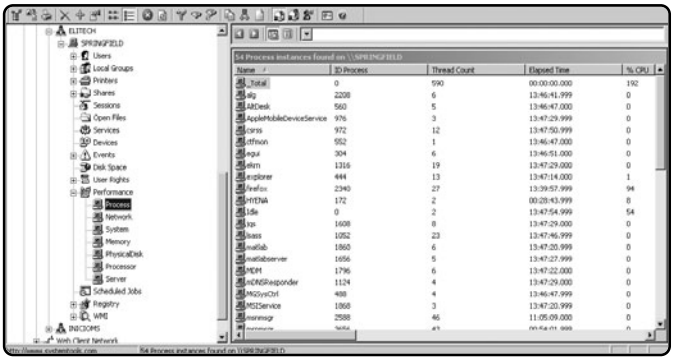


FIGURA 14.
Hyena es una herramienta que permite realizar enumeración de distintos equipos dentro de una red.

Una vez encontrada una vulnerabilidad, el atacante buscará un **exploit** que le permita explotarla y obtener el control, lo que en la jerga se conoce como **ownear el servidor**. Este proceso puede llevarse a cabo en forma manual o mediante algún sistema de **explotación**. Algunos de estos son **Metasploit Framework** (**www.metasploit.org**), **Core Impact** (**www.coresecurity.com**) o **Immunity Canvas** (**www.immunitysec.com**). En la actualidad, existen varios recursos online donde podemos conseguir exploits e información sobre vulnerabilidades, como Milw0rm (**www.milw0rm.com**) (**Figura 15**), Open Source Vulnerability Database (**http://osvdb.org**), Bugtraq (**www.securityfocus.com/archive/1**), Packet storm (**www.packetstormsecurity.org**) y BugReport (**www.bugreport.ir**).

También podemos mencionar Common Vulnerability Scoring System (**www.first.org/cvss**) y Common Vulnerabilities and Exposures (**http://cve.mitre.org**)

Según el tipo de exploit ejecutado, puede ser que el acceso conseguido no posea los privilegios elevados que el atacante desee, y será necesario emprender

Una vez detectadas las vulnerabilidades, el gran paso es el ingreso al sistema definido como objetivo

EL EFECTO FISIOLÓGICO

En el momento del ataque (aunque sea simulado), la sensación y la adrenalina son tan altas que, en ocasiones, el atacante siente el sudor frío propio de los momentos de máximo estrés, previo a cumplir el objetivo que lo llenará de satisfacción.

FIGURA 15.
Milw0rm es un sitio que brinda información de primera mano sobre las últimas vulnerabilidades.

una **escalada de privilegios**, con el objetivo de poseer control total del sistema atacado. Una de las formas más comunes de escalar privilegios es, a partir del ingreso al sistema, usar otro exploit (en este caso local) que otorgue privilegios de administrador (**`root`** para Unix/Linux, o **`Administrador`** o **`System`** para sistemas Windows).

Una vez que se obtuvo una cuenta con altos privilegios, el siguiente paso suele ser ejecutar comandos o aplicaciones en forma remota. Es decir, lanzar una aplicación desde la ubicación del atacante y que ésta se ejecute en el sistema comprometido. Para esto, es necesario haber establecido previamente un canal entre ambos equipos. Por ejemplo, una vez establecido el canal, podemos ejecutar aplicaciones en forma remota mediante la aplicación **PsExec** de **Sysinternals** (**http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx**).

Una alternativa a la forma de acceso planteada es hacer que el **usuario** que está en el equipo objetivo **intervenga** de forma tal que facilite nuestro objetivo. Muchas veces, esto es necesario ya que se simplifica la explotación o bien no es posible ejecutar remotamente el exploit. En estos casos, se suele engañar al usuario mediante técnicas de **ingeniería social**, solicitándole por algún medio (e-mail, mensajería instantánea, etcétera) que realice una determinada acción. Lo que el usuario no sabe es que esa acción explota una vulnerabilidad y brinda acceso remoto al atacante.

EXPLOIT

La palabra **exploit** proviene del inglés, y en español significa **explotar** o **aprovechar**. En informática, es una porción de software, fragmento de datos o secuencia de comandos que aprovecha un error intencionalmente, a fin de causar un comportamiento no deseado.

FASE DE MANTENIMIENTO DEL ACCESO

Una vez obtenido el acceso, lo que realmente se desea es mantener al equipo comprometido entre las filas del atacante. Para esto, hay que buscar la manera de que el acceso ganado sea perdurable en el tiempo.

En la mayoría de los casos, esto se logra a partir de la instalación y la ejecución de diversos tipos de **software malicioso**. Si bien el comportamiento va a cambiar dependiendo del tipo de software, el resultado siempre es el mismo: el atacante podrá retomar el acceso al equipo comprometido cada vez que lo desee.

Algunos ejemplos del software que se utiliza en esta etapa son los **troyanos** y **backdoors**, **keyloggers**, **spyware**, etcétera.

Retomando la planificación del ataque, ya mencionamos que siempre se busca mantener la **anonimidad** en el ataque y, por otro lado, ocultar huellas. En esta fase, el atacante buscará lo mismo. Intentará, con mayor o menor suerte, no dejar rastros de su paso y también esconder los medios por los cuales mantiene el acceso al equipo comprometido.

En Internet hay varios sitios donde podemos encontrar información sobre Penetration Testing. Algunos de ellos son: **www.isecom.org/osstmm**, **http://csrc.nist.gov**, **www.oissg.org** y también **www.vulnerabilityassessment.co.uk**. Una de las metodologías más reconocidas es la **OSSTMM** (*Open Source Security Testing Methodology Manual*), que especifica en forma detallada los pasos necesarios para llevar adelante un Penetration Test (**Figura 16**).

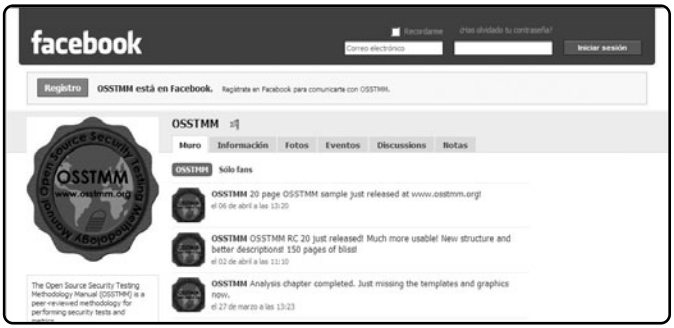


FIGURA 16.
En la imagen podemos ver el grupo de la OSSTMM **en la popular red social** Facebook**.**

RESUMEN

En este capítulo, hemos repasado conceptos relacionados con la seguridad informática y resumimos algunos tipos de evaluaciones de seguridad, como Vulnerability Assessment, Penetration Test y Ethical Hacking. También, analizamos en detalle las fases de un Pentest.

Multiple **choice**

1 ¿Cuál de los siguientes conceptos no pertenece a la tríada CIA?
a- Calidad.
b- Confidencialidad.
c- Integridad.
d- Disponibilidad.

2 ¿Cuál de las siguientes opciones no es un concepto que podamos asociar a la tríada CIA?
a- Identificación.
b- Autorización.
c- Invunerabilidad.
d- Autenticación.

3 ¿Cuál de los siguientes conceptos nos indica que toda modificación de la información solo es realizada por usuarios autorizados, por medio de procesos autorizados?
a- Calidad.
b- Confidencialidad.
c- Integridad.
d- Disponibilidad.

4 ¿Cuál es la primera fase de un Penetration Test?
a- Reconocimiento.
b- Enumeración.
c- Escaneo.
d- Acceso.

5 ¿Cuál es la segunda fase de un Penetration Test?
a- Reconocimiento.
b- Enumeración.
c- Escaneo.
d- Acceso.

6 ¿Cuál es la tercera fase de un Penetration Test?
a- Reconocimiento.
b- Enumeración.
c- Escaneo.
d- Acceso.

Respuestas: 1-a, 2-c, 3-b, 4-a, 5-c, 6-b.

Capítulo 9

Metodologías de análisis

En este apéndice, conoceremos todo sobres las metodologías de análisis: OSSTMM, ISSAF, OWASP.

Metodologías de análisis

Las metodologías funcionan como guías para realizar determinados objetivos, e implican una serie de métodos. Se dice que un método es el procedimiento para alcanzar el objetivo, y la metodología es el estudio del método en sí.

Aplicado este concepto al análisis de seguridad, se refiere a las distintas maneras de conseguir los resultados de un testeo de manera organizada y de común acuerdo entre distintos profesionales. En este caso, veremos tres referencias metodológicas muy utilizadas, cada una con su nivel de madurez propio.

OSSTMM

Open Source Security Testing Methodology Manual (**OSSTMM**, cuya página web es **www.isecom.org/osstmm**) es un **manual de metodología abierta para pruebas de seguridad**, que ha marcado un hito en la historia de este ambiente. Si bien es cierto que los tests individuales que se mencionan no son particularmente revolucionarios, la metodología representa un estándar de referencia imprescindible para todo aquél que quiera llevar a cabo un testeo de seguridad en forma ordenada y profesional. Comprende gran parte de los aspectos que debemos tener en cuenta al momento de realizar pruebas de seguridad, y a fin de organizar su contenido, se encuentra dividido en varias secciones.

Del mismo modo, es posible identificar en él una serie de módulos de testeo específicos, a través de los cuales se observan cada una de las dimensiones de seguridad, integradas con las tareas a llevar a cabo en los diferentes puntos de revisión.

Los temas abarcados son **seguridad de la información**, **seguridad de los procesos**, **seguridad en las tecnologías de Internet**, **seguridad en las comunicaciones**, **seguridad inalámbrica** y **seguridad física**. La guía ayuda a determinar qué hay que hacer, cómo hay que hacerlo y cuándo hay que hacerlo. De esta forma, tenemos la certeza de que vamos a estar siguiendo una metodología probada a la hora de evaluar una postura

Las metodologías funcionan como guías para realizar determinados objetivos, e implican una serie de métodos

respecto de la seguridad y que esto no se convertirá en un juego de azar (**Figura 1**).

OSSTMM no solo abarca los ámbitos técnicos y de operación de seguridad tradicionales, sino que también se encarga de definir aspectos tales como las credenciales del profesional a cargo del test, la forma en la que el test debe ser comercializado, la manera en la que los resultados de éste deben ser presentados, las normas éticas y legales que deben tenerse en cuenta al momento de concretar el test, los tiempos probables para cada una de las tareas y, por sobre toda las cosas, incorpora el concepto de **Valor de Evaluación de Riesgo** (**RAV**) y, con él, la frecuencia con la que el test tiene que ser ejecutado. Se aplican los siguientes términos a los diferentes tipos de sistemas y de tests de seguridad de redes, basados en tiempo y costo (**Figura 2**).

1) **Búsqueda de vulnerabilidades**: Usualmente, se refiere a las comprobaciones automáticas de un sistema o sistemas dentro de una red.

FIGURA 1. El logo de OSSTMM (Open Source Security Testing Methodology Manual) es fácilmente reconocible y permite identificar el uso de la metodología.

2) **Escaneo de la seguridad**: En general, se refiere a las búsquedas de vulnerabilidades que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles de la red y análisis profesional individualizado.

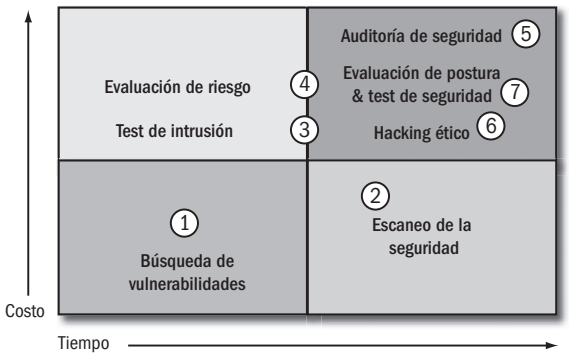


FIGURA 2. En este diagrama, podemos observar la relación de tiempos contra costos y las pruebas asociadas que mencionamos anteriormente.

3) Test de intrusión: Generalmente, se refiere a los proyectos orientados a objetivos en los cuales la meta es obtener un trofeo, que incluye ganar acceso privilegiado con medios precondicionales.

4) Evaluación de riesgo: Se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio, que incluyen la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.

5) Auditoria de seguridad: Hace referencia a la inspección manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema dentro de una red o redes.

6) Hacking ético: Usualmente, se refiere a los tests de intrusión en los cuales el objetivo es obtener trofeos en la red dentro del tiempo predeterminado de duración del proyecto.

7) Test de seguridad: Y su equivalente militar, **Evaluación de postura**, es una evaluación de riesgo con orientación de proyecto de los sistemas y redes, a través de la aplicación de análisis profesional mediante escaneos de seguridad, donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto.

FASES QUE COMPONEN OSSTMM

- **Seccion A:**
  Seguridad de la información
  01. Revisión de la inteligencia competitiva.
  02. Revisión de privacidad.
  03. Recolección de documentos.

- **Seccion B:**
  Seguridad de los procesos
  01. Testeo de solicitud.

La intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos

02. Testeo de sugerencia dirigida.
03. Testeo de las personas confiables.

- **Seccion C:**
  Seguridad en las tecnologías de Internet
  01. Logística y controles.
  02. Exploración de red.
  03. Identificación de los servicios del sistema.
  04. Búsqueda de información competitiva.
  05. Revisión de privacidad.
  06. Obtención de documentos.
  07. Búsqueda y verificación de vulnerabilidades.
  08. Testeo de aplicaciones de internet.
  09. Enrutamiento.
  10. Testeo de sistemas confiados.
  11. Testeo de control de acceso.
  12. Testeo de sistema de detección de intrusos.
  13. Testeo de medidas de contingencia.

14. Descifrado de contraseñas.
15. Testeo de denegación de servicios.
16. Evaluación de políticas de seguridad.

- **Seccion D:**
  Seguridad en las comunicaciones
  01. Testeo de PBX.
  02. Testeo del correo de voz.
  03. Revisión del fAX.
  04. Testeo del módem.

- **Seccion E:**
  Seguridad inalámbrica
  01. Verificación de radiación electromagnética (EMR).
  02. Verificación de redes inalámbricas [802.11].
  03. Verificación de redes bluetooth.
  04. Verificación de dispositivos de entrada inalámbricos.
  05. Verificación de dispositivos de mano inalámbricos.
  06. Verificación de comunicaciones sin cable.
  07. Verificación de dispositivos de vigilancia inalámbricos.
  08. Verificación de dispositivos de transacción inalámbricos.
  09. Verificación de RFID.
  10. Verificación de sistemas infrarrojos.
  11. Revisión de privacidad.

- **Seccion F:**
  Seguridad física
  01. Revisión de perímetro.
  02. Revisión de monitoreo.
  03. Evaluación de controles de acceso.
  04. Revisión de respuesta de alarmas.
  05. Revisión de ubicación.
  06. Revisión de entorno.

ISSAF

Information System Security Assessment Framework (**ISSAF**) es un proyecto de *Open Information System Security Group* (**OISSG**, cuya página web es **www.oissg.org**). Constituye un marco de trabajo detallado respecto de las prácticas y conceptos relacionados con todas y cada una de las tareas que debemos realizar al conducir un testeo de seguridad.

La información contenida en ISSAF (**Figura 3**) se encuentra organizada alrededor de lo que se ha dado en llamar **criterios de evaluación**, cada uno de los cuales ha sido escrito y revisado por expertos en cada una de las áreas de aplicación. Estos criterios de evaluación, a su vez, se componen de los siguientes ítems:

- Una descripción del criterio de evaluación.
- Puntos y objetivos para cubrir.
- Los prerrequisitos para conducir la evaluación.
- El proceso mismo de evaluación.
- El informe de los resultados esperados.
- Las contramedidas y recomendaciones.
- Referencias y documentación externa.

La información contenida en ISSAF se encuentra organizada alrededor de lo que se ha dado en llamar criterios de evaluación

A fin de establecer un orden preciso y predecible, dichos criterios se encuentran contenidos dentro de diferentes dominios entre los que es posible encontrar, desde los aspectos más generales, como ser los conceptos básicos de la administración de proyectos de testeo de seguridad, hasta técnicas tan puntuales como la ejecución de pruebas de inyección de código **SQL** o las estrategias de cracking.

Los reportes de ejemplo, plantillas de seguimiento de proyecto, plantillas de contratos de trabajo/confidencialidad (*Security Assessment Contract/NDA: Non-Disclosure Agreement*), listas de verificación, testeo del software antivirus, armado del laboratorio de pruebas y muchos aspectos más completan la primera edición que, si bien aún no se encuentra finalizada en su totalidad a la fecha, brinda información detallada acerca de las tareas que debe realizar el encargado de testear la seguridad.

Lo último es de suma importancia, puesto que el alto nivel de detalle y su estrecha e inevitable

FIGURA 3. Logo de ISSAF (Information System Security Assessment Framework), el ambicioso proyecto de referencia para evaluaciones de seguridad.

Open Web Application Security Project (OWASP, cuya web es www.owasp.org) es un proyecto centrado en la seguridad sobre aplicaciones web

relación con el **software**, **plataforma** o **tecnología** hacen que la actualización sea una desventaja respecto a otras metodologías más generales. Esto no debemos considerarlo un inconveniente, sino un punto que hay que tener en cuenta a la hora utilizar el sistema.

OWASP

Open Web Application Security Project (**OWASP**, cuya web es **www.owasp.org**) es un proyecto centrado en la seguridad sobre aplicaciones web, que está conformado por una comunidad abierta y libre cuya misión es hacer visible y consciente a la seguridad en aplicaciones, de manera que las organizaciones puedan tomar mejores decisiones sobre sus riesgos de seguridad (**Figura 4**).

Todo el material está disponible bajo una licencia de software libre y abierto. La fundación OWASP es una asociación sin fines de lucro. La comunidad está formada por empresas, organizaciones educativas y particulares de todo el mundo, que crean artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser usadas libre y gratuitamente. El proyecto se inició en el año 2000, y la fundación se creó en 2004 para apoyar los proyectos e infraestructura de OWASP. Para su mantenimiento depende de las donaciones y cuotas de los socios, particulares y empresas.

Los líderes de OWASP son responsables de tomar decisiones sobre la dirección técnica, las prioridades del proyecto, los plazos y las publicaciones. OWASP no está afiliado a ninguna compañía tecnológica, si bien apoya el uso informado de tecnologías de seguridad. Recomienda enfocar la seguridad de aplicaciones informáticas considerando todas sus dimensiones: **personas**, **procesos** y **tecnologías**. Los proyectos OWASP se dividen en dos categorías principales, proyectos de desarrollo y de documentación. Los proyectos de documentación actuales son los siguientes:

- **Guía de desarrollo**: un documento que nos proporciona una guía detallada para construir aplicaciones web seguras.

- **Guía de pruebas**: una guía centrada en las pruebas y listas de comprobación de seguridad sobre aplicaciones web.
- **Top 10**: un documento de concienciación sobre las vulnerabilidades críticas de las aplicaciones web.
- **Legal**: un proyecto centrado en la contratación de servicios de software y sus aspectos de seguridad.
- **AppSec FAQ**: respuestas a las preguntas más frecuentes sobre seguridad de aplicaciones web.

Entre los proyectos de desarrollo, se incluyen **WebScarab**, una aplicación para realizar pruebas de seguridad en aplicaciones y servicios web, y **WebGoat**, un entorno de entrenamiento para que los usuarios aprendan sobre seguridad de aplicaciones web de forma segura y legal.

En este caso nos enfocaremos en la guía de pruebas, que presenta justamente una metodología para llevar a cabo los tests de seguridad. El framework se refiere a 5 fases, la anterior al desarrollo, la de definición y diseño, la del tiempo en que se realiza el desarrollo, la del tiempo de instalación y publicación y la de mantenimiento y operaciones.

FIGURA 4. **El logo de** OWASP **(Open Web Application Security Project), el gran proyecto centrado en la seguridad sobre aplicaciones web.**

En cuanto a las pruebas, se divide en:

- Obtención de información.
- Pruebas de reglas de negocio.
- Pruebas de autenticación.
- Pruebas de manejo de sesión.
- Pruebas de validación de datos.
- Pruebas de denegación de servicio (DoS).
- Pruebas en servicios web.
- Pruebas en AJAX.

Multiple **choice**

1 ¿Cómo se denomina la inspección manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema dentro de una red o redes?

a- Test de intrusión.
b- Auditoria de seguridad.
c- Test de seguridad.
d- Evaluación de riesgo.

2 ¿Cómo se denominan los proyectos orientados a objetivos en los cuales la meta es obtener un trofeo, que incluye ganar acceso privilegiado con medios precondicionales?

a- Test de intrusión.
b- Auditoria de seguridad.
c- Test de seguridad.
d- Evaluación de riesgo.

3 ¿Cómo se denominan los análisis de seguridad a través de entrevistas e investigación de nivel medio?

a- Test de intrusión.
b- Auditoria de seguridad.
c- Test de seguridad.
d- Evaluación de riesgo.

4 ¿Cuál de los siguientes proyectos OWASP un proyecto centrado en la contratación de servicios de software y sus aspectos de seguridad?

a- Legal.
b- AppSec FAQ.
c- WebGoat.
d- Top 10.

5 ¿Cuál de los siguientes proyectos OWASP es un documento de concienciación sobre las vulnerabilidades críticas de las aplicaciones web?

a- Legal.
b- AppSec FAQ.
c- WebGoat.
d- Top 10.

6 ¿Cuál de los siguientes proyectos OWASP no corresponde a una función de documentación?

a- Legal.
b- AppSec FAQ.
c- WebGoat.
d- Top 10.

Respuestas: 1-b, 2-a, 3-d, 4 -a, 5-d, 6-c.

Servicios **al lector**

Encontraremos información adicional relacionada con el contenido que servirá para complementar lo aprendido.

Índice **temático**

A

B

C

D

E

F

G

H

I

K

L

M

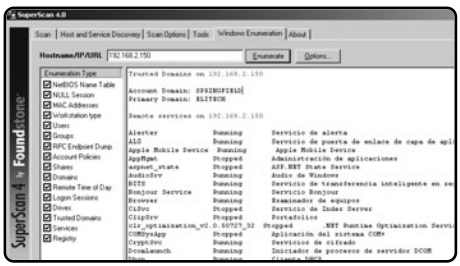
N

O

P

R

S



T

V

W

X

Sitios web **recomendados**

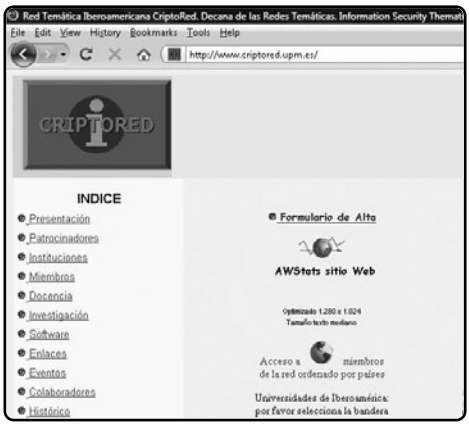
SEGU INFO
www.segu-info.com.ar

Blog argentino con información de primer nivel, noticias de actualidad, eventos, descarga de herramientas y foro de discusión. Se destaca la calidad y cantidad de profesionales que colaboran y el impecable trabajo de su creador, el licenciado Christian Borghello.

SECURITY FOCUS
www.securityfocus.com

Uno de los sitios de mayor prestigio del mundo. Posee listas de correo por temáticas, como Microsoft, Unix, Forense e ISO 27001, entre otras. Se recomienda no suscribirse en principio a todas las listas, ya que la información puede ser excesiva.

CRIPTO RED
www.criptored.upm.es



Sitio de la **Red Temática Iberoamericana de Criptografía** y Seguridad de la Información de la **Universidad Politécnica de Madrid**. Ofrece material educativo, calendario de eventos, descarga de charlas, videos y material de presentaciones.

HISPASEC
www.hispasec.com

Un interesante sitio en español, con un detalle de gran utilidad, que es la lista de correo **una-al-dia**, donde a todos los suscriptores les llega diariamente un correo con una noticia de seguridad.

KRIPTÓPOLIS
www.kriptopolis.org

Blog en castellano, dedicado a temas de criptografía y seguridad en general. Además, posee distintos foros y la posibilidad de hacer consultas. También, se pueden encontrar tutoriales y enlaces a material educativo en general.

MICROSOFT TECHNET SECURITY CENTER
http://technet.microsoft.com/security

Portal de seguridad de Microsoft con gran cantidad de recursos para estos sistemas. Posee una sección con boletines sobre seguridad, descargas y eventos. El sitio sólo está disponible en inglés.

LINUX SECURITY
www.linuxsecurity.com

Bajo el lema de The central voice for Linux and Open Source security news, este sitio en inglés ofrece una variedad interesante de recursos de seguridad para plataformas Linux.

SECURITY TUBE
www.securitytube.net

Un sitio al mejor estilo **YouTube**, pero donde el contenido tiene relación con la seguridad informática. Pueden encontrarse videos y tutoriales categorizados para aprendizaje de técnicas y uso de herramientas.

SECURITEAM
www.securiteam.com

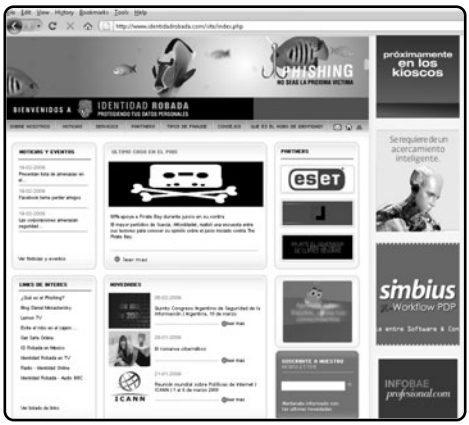
Sitio en inglés dedicado a la divulgación de noticias, alertas de seguridad, exploits y herramientas. También ofrece suscripción gratuita para recibir la información por e-mail o RSS.

SANS INSTITUTE
www.sans.org

SANS Institute es referencia en cuanto a capacitación y certificaciones de seguridad. El sitio ofrece información respecto a las capacitaciones, certificaciones, eventos y el famoso **Top 20 de las vulnerabilidades**.

IDENTIDAD ROBADA

www.identidadrobada.com



Sitio dedicado a la problemática del robo de identidad. Aquí se podrán encontrar noticias relacionadas, documentos y consejos para evitar ser víctimas de este tipo de fraude tan común en la actualidad.

ARCERT

www.arcert.gov.ar

ArCERT es una unidad de respuesta a incidentes de seguridad para organismos de la administración pública de la Argentina. Ofrece gran cantidad de enlaces de interés y material de referencia.

CCCURE
www.cccure.org

En este sitio puede encontrarse gran cantidad de recursos para preparar el examen de la certificación CISSP, como ser videos, documentos, modelos de examen y otros.

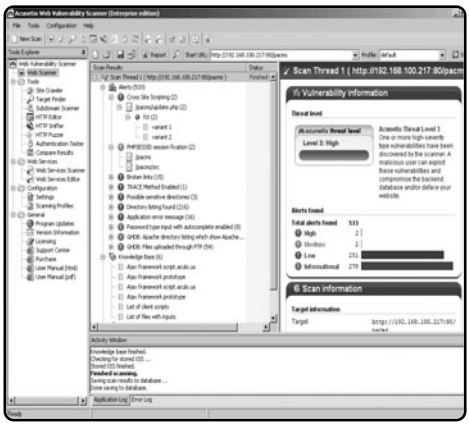
ROMPECADENAS
www.rompecadenas.com.ar

Este sitio se especializa en desmitificar historias y esclarecer la realidad sobre las cadenas de e-mail que llegan como spam y otros temas relacionados como el phishing y el malware.

Programas **útiles**

ACUNETIX WEB VULNERABILITY SCANNER

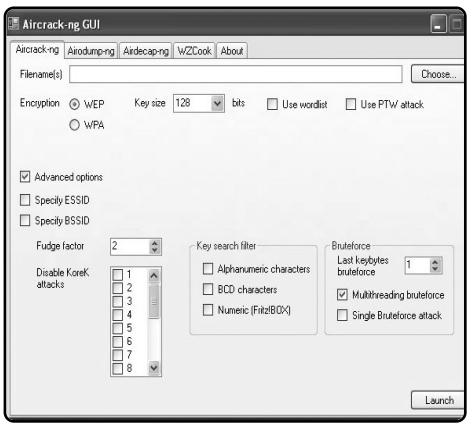
www.acunetix.com



Acunetix es un escáner de vulnerabilidades especialmente diseñado para auditar sistemas web. Cuenta con un poderoso generador de reportes y tiene una interfaz muy amigable.

AIRCRACK

www.aircrack-ng.org



Aircrack es una herramienta multiplataforma, liberada bajo licencia GPL, que permite auditar la seguridad de los sistemas y los protocolos inalámbricos, con distintos niveles de cifrado.

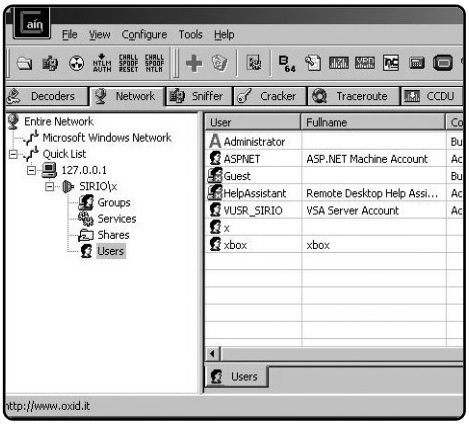
BACKTRACK

www.remote-exploit.org

BackTrack es una distribución LiveCD de Linux orientada a la seguridad, que incluye una gran cantidad de herramientas para realizar pruebas de penetración de sistemas.

CAIN Y ABEL

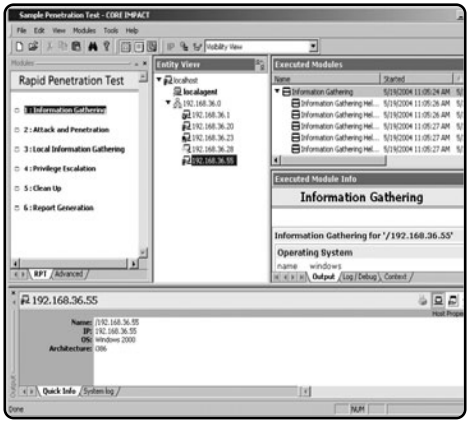
www.oxit.it



Cain y Abel es un completo software de seguridad que incluye diversas herramientas de auditoría de redes y contraseñas. También cuenta con varias utilidades para análisis de protocolos.

CORE IMPACT

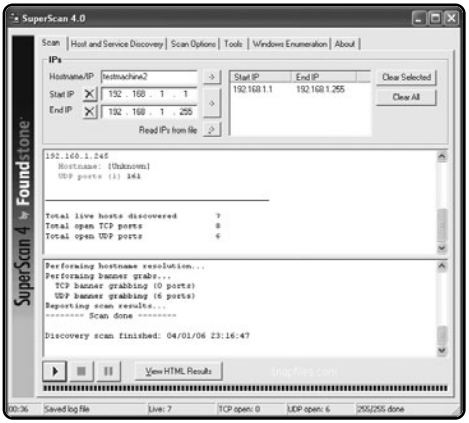
www.coresecurity.com



Core Impact es un poderoso sistema de explotación de vulnerabilidades con gran cantidad de funcionalidades y una interfaz gráfica muy depurada e intuitiva.

FOUNDSTONE TOOLS

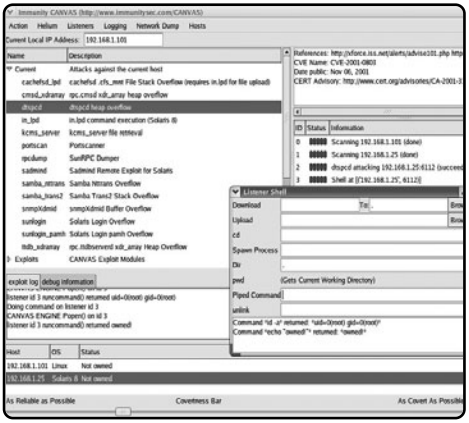
www.foundstone.com/us/resources-free-tools.asp



Es una serie de utilidades de auditoría de sistemas y seguridad, desarrolladas por Foundstone, y organizadas en distintas categorías. Tienen la característica de ser gratuitas.

IMMUNITY CANVAS

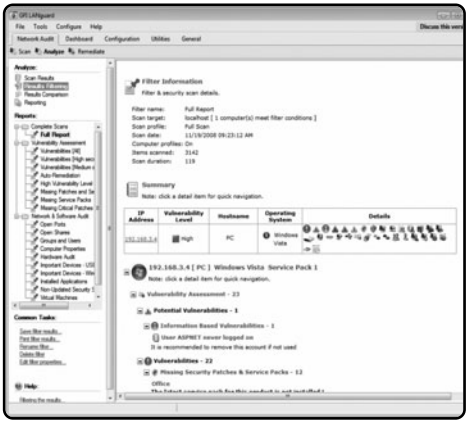
www.immunityc.com



CANVAS es un sistema de explotación de vulnerabilidades que funciona en una gran cantidad de sistemas y aplicaciones, e incluye cientos de exploits listos para ser utilizados.

LANGUARD

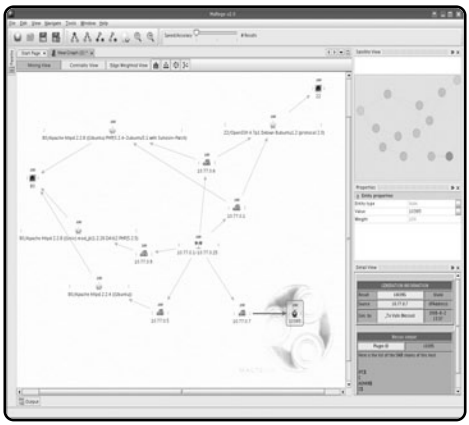
www.gfi.com/languard



LANguard es un clásico escáner de vulnerabilidades de la empresa GFI, que brinda la posibilidad de realizar la instalación automática de parches en sistemas Windows.

MALTEGO

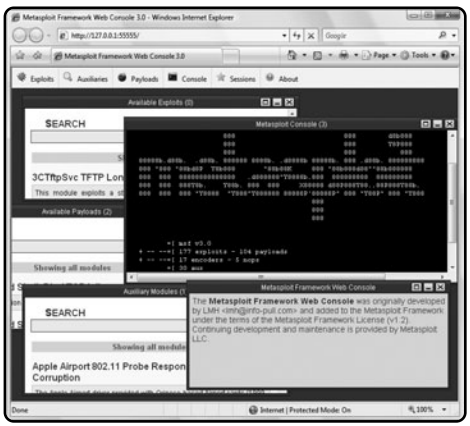
www.paterva.com/maltego



Maltego es una herramienta de inteligencia que facilita la recopilación y la representación de información. Además, con ella es posible comparar datos y determinar las relaciones desconocidas.

METASPLOIT FRAMEWORK

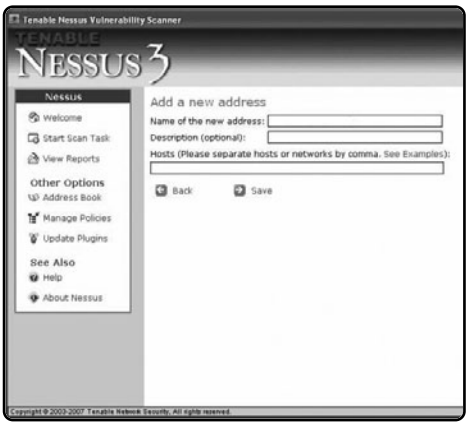
www.metasploit.org



Metasploit es un framework de explotación de vulnerabilidades con licencia libre que permite lanzar ataques y obtener una consola remota del sistema atacado. También posee una base de datos de opcodes y shellcodes.

NESSUS

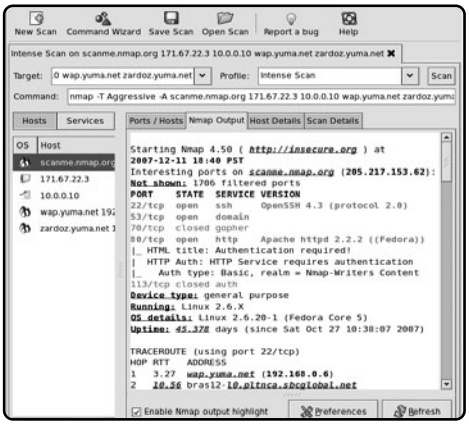
www.nessus.org



Nessus es uno de los escáneres de vulnerabilidades más utilizados. Funciona con actualización de plugins para la detección de debilidades existentes y utiliza una arquitectura cliente-servidor.

NMAP

www.insecure.org



NMap es el escáner de puertos por excelencia. Creado por Fyodor, y mantenido por una gran comunidad de software libre, posee funciones de averiguación de sistemas operativos y opera con prácticamente todas las modalidades de escaneo conocidas.

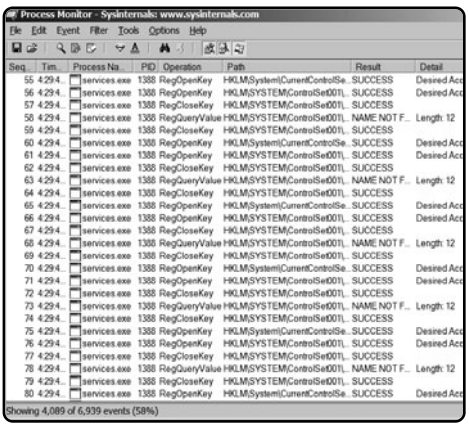
OWASP LIVECD

www.owasp.org

Es una distribución LiveCD de Linux desarrollada por la comunidad del proyecto OWASP, que cuenta con una gran cantidad de herramientas de auditoría y seguridad para entornos web.

SYSINTERNALS SUITE

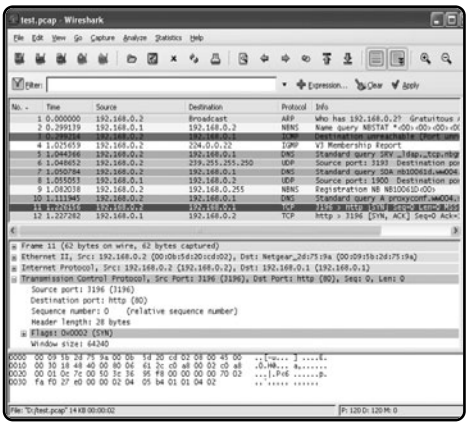
www.microsoft.com/sysinternals



Sysinternals Suite es un set de herramientas de auditoría y monitoreo de sistemas Windows. En la actualidad posee alrededor de 60 utilidades para diferentes tareas de administración y seguridad.

WIRESHARK

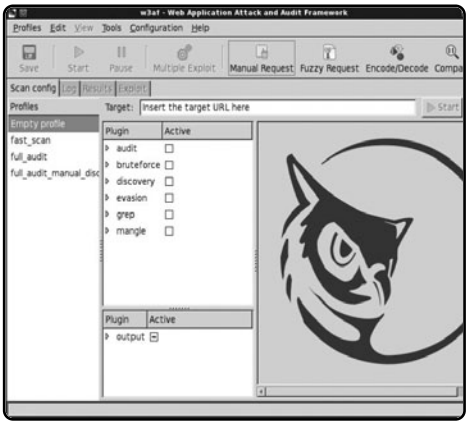
www.wireshark.org



Wireshark es el programa de análisis de protocolos por excelencia, que proviene del antiguo proyecto Ethereal. Permite estudiar los paquetes de red y analizar los flujos de datos de una gran variedad de protocolos.

W3AF

http://w3af.sourceforge.net

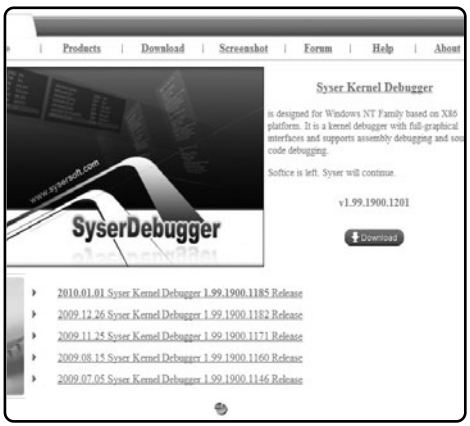


W3AF es un framework de explotación de vulnerabilidades orientado a sistemas web, con licencia GPL, que posibilita incluir plugins propios y cuenta con una gran cantidad de ellos disponibles, desarrollados por su creador.

ULTRAEDIT
www.ultraedit.com

Ultraedit es un editor de archivos ejecutables. Muy utilizado por programadores de todos los lenguajes y plataformas, como XML, HTML, PHP, Java, Javascript y otros. Cuenta con más de 2 millones de usuarios en todo el mundo.

SYSERDEBUGGER
www.sysersoft.com



Es un debugger de Kernel con una interfaz completamente gráfica. Una elección muy completa para realizar todo tipo de tareas relacionadas debido a que es uno de los programas que brinda más cantidad de opciones al programador.

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 hasta un CD-ROM, desde un Servicio de Atención al Lector hasta la posibilidad de leer el sumario en la Web para evaluar con tranquilidad la compra, o la presencia de adecuados índices temáticos, todo suma al valor de un buen libro.

5 VERIFIQUE EL IDIOMA

No sólo el del texto; también revise que las pantallas incluidas en el libro estén en el mismo idioma del programa que usted utiliza.

6 REVISE LA FECHA DE PUBLICACIÓN

Está en letra pequeña en las primeras páginas; si es un libro traducido, la que vale es la fecha de la edición original.

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 **

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

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

Photoshop

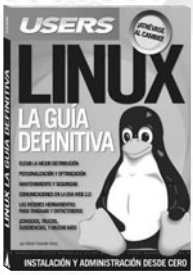
En este libro aprenderemos sobre las más novedosas técnicas de edición de imágenes en Photoshop. El autor nos presenta de manera clara y práctica todos los conceptos necesarios, desde la captura digital hasta las más avanzadas técnicas de retoque.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1773-05-3

Grabación y producción de música

En este libro repasaremos todos los aspectos del complejo mundo de la producción musical. Desde las cuestiones para 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 migrar 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

Premiere + After Effects

Esta obra nos presenta un recorrido detallado por las aplicaciones audiovisuales de Adobe: Premiere Pro, After Effects y Soundbooth. Todas las técnicas de los profesionales, desde la captura de video hasta la creación de efectos, explicadas de forma teórica y práctica.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-26013-9-3

Office 2010

En este libro aprenderemos a utilizar todas las aplicaciones de la suite, en su versión 2010. Además, su autora nos mostrará las novedades más importantes, desde los minigráficos de Excel hasta Office Web Apps, todo presentado en un libro único.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-26013-6-2

Excel Paso a Paso

En esta obra encontraremos una increíble selección de proyectos pensada para aprender mediante la práctica la forma de agilizar todas las tareas diarias. Todas las actividades son desarrolladas en procedimientos paso a paso de una manera didáctica y fácil de comprender.

→ COLECCIÓN: PASO A PASO
→ 320 páginas / ISBN 978-987-26013-4-8

¡Léalo antes Gratis!

En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.

C#

Este libro es un completo curso de programación con C# actualizado a la versión 4.0. Ideal tanto para quienes desean migrar a este potente lenguaje, como para quienes quieran aprender a programar desde cero en Visual Studio 2010.

→ COLECCIÓN: MANUALES USERS
→ 400 páginas / ISBN 978-987-26013-5-5

200 Respuestas Seguridad

Esta obra es una guía básica que responde, en forma visual y práctica, a todas las preguntas que necesitamos contestar para conseguir un equipo seguro. Definiciones, consejos, claves y secretos, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-26013-1-7

Funciones en Excel

Este libro es una guía práctica de uso y aplicación de todas las funciones de la planilla de cálculo de Microsoft. Desde las funciones de siempre hasta las más complejas, todas presentadas a través de ejemplos prácticos y reales.

→ COLECCIÓN: MANUALES USERS
→ 368 páginas / ISBN 978-987-26013-0-0

Proyectos con Windows 7

En esta obra aprenderemos cómo aprovechar al máximo todas las ventajas que ofrece la PC. Desde cómo participar en las redes sociales hasta las formas de montar una oficina virtual, todo presentado en 120 proyectos únicos.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-036-8

PHP 6

Este libro es un completo curso de programación en PHP en su versión 6.0. Un lenguaje que se destaca tanto por su versatilidad como por el respaldo de una amplia comunidad de desarrolladores, que lo convierten en un punto de partida ideal para quienes comienzan a programar.

→ COLECCIÓN: MANUALES USERS
→ 368 páginas / ISBN 978-987-663-039-9

200 Respuestas: Blogs

Esta obra es una completa guía que responde a las preguntas más frecuentes de la gente sobre la forma de publicación más poderosa de la Web 2.0. Definiciones, consejos, claves y secretos, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: 200 RESPUESTAS
→ 320 páginas / ISBN 978-987-663-037-5

Hardware paso a paso

En este libro encontraremos una increíble selección de actividades que abarcan todos los aspectos del hardware. Desde la actualización de la PC hasta el overclocking de sus componentes, todo en una presentación nunca antes vista, realizada íntegramente con procedimientos paso a paso.

→ COLECCIÓN: PASO A PASO
→ 320 páginas / ISBN 978-987-663-034-4

200 Respuestas: Windows 7

Esta obra es una guía básica que responde, en forma visual y práctica, a todas las preguntas que necesitamos conocer para dominar la última versión del sistema operativo de Microsoft. Definiciones, consejos, claves y secretos, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: 200 RESPUESTAS
→ 320 páginas / ISBN 978-987-663-035-1

Office paso a paso

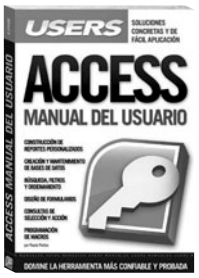
Este libro presenta una increíble colección de proyectos basados en la suite de oficina más usada en el mundo. Todas las actividades son desarrolladas con procedimientos paso a paso de una manera didáctica y fácil de comprender.

→ COLECCIÓN: PASO A PASO
→ 320 páginas / ISBN 978-987-663-030-6

101 Secretos de Hardware

Esta obra es la mejor guía visual y práctica sobre hardware del momento. En su interior encontraremos los consejos de los expertos sobre las nuevas tecnologías, las soluciones a los problemas más frecuentes, cómo hacer overclocking, modding, y muchos más trucos y secretos.

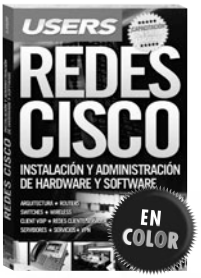
→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-029-0



Access

Este manual nos introduce de lleno en el mundo de Access para aprender a crear y administrar bases de datos de forma profesional. Todos los secretos de una de las principales aplicaciones de Office, explicados de forma didáctica y sencilla.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-025-2



Redes Cisco

Este libro permitirá al lector adquirir todos los conocimientos necesarios para planificar, instalar y administrar redes de computadoras. Todas las tecnologías y servicios Cisco, desarrollados de manera visual y práctica en una obra única.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-024-5

¡Léalo antes Gratis!

En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.

Proyectos con Office

Esta obra nos enseña a usar las principales herramientas de Office a través de proyectos didácticos y útiles. En cada capítulo encontraremos la mejor manera de llevar adelante todas las actividades del hogar, la escuela y el trabajo.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-023-8

Dreamweaver y Fireworks

Esta obra nos presenta las dos herramientas más poderosas para la creación de sitios web profesionales de la actualidad. A través de procedimientos paso a paso, nos muestra cómo armar un sitio real con Dreamweaver y Fireworks sin necesidad de conocimientos previos.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-022-1

Excel revelado

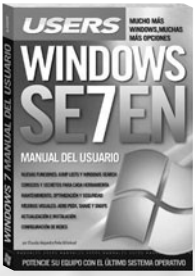
Este manual contiene una selección de más de 150 consultas de usuarios de Excel y todas las respuestas de Claudio Sánchez, un reconocido experto en la famosa planilla de cálculo. Todos los problemas encuentran su solución en esta obra imperdible.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-021-4

Robótica avanzada

Esta obra nos permitirá ingresar al fascinante mundo de la robótica. Desde el ensamblaje de las partes hasta su puesta en marcha, todo el proceso está expuesto de forma didáctica y sencilla para así crear nuestros propios robots avanzados.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-020-7



Windows 7

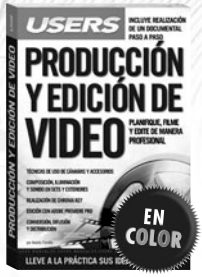
En este libro encontraremos las claves y los secretos destinados a optimizar el uso de nuestra PC tanto en el trabajo como en el hogar. Aprenderemos a llevar adelante una instalación exitosa y a utilizar todas las nuevas herramientas que incluye esta versión.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-015-3

De Windows a Linux

Esta obra nos introduce en el apasionante mundo del software libre a través de una completa guía de migración, que parte desde el sistema operativo más conocido: Windows. Aprenderemos cómo realizar gratuitamente aquellas tareas que antes hacíamos con software pago.

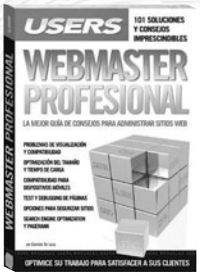
→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-013-9



Producción y edición de video

Un libro ideal para quienes deseen realizar producciones audiovisuales con bajo presupuesto. Tanto estudiantes como profesionales encontrarán cómo adquirir las habilidades necesarias para obtener una salida laboral con una creciente demanda en el mercado.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-012-2



Webmaster Profesional

Esta obra explica cómo superar los problemas más frecuentes y complejos que enfrenta todo administrador de sitios web. Ideal para quienes necesiten conocer las tendencias actuales y las tecnologías en desarrollo que son materia obligada para dominar la Web 2.0.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-011-5

Silverlight

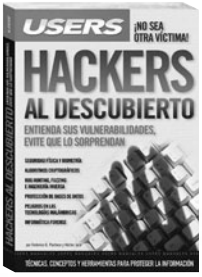
Este manual nos introduce en un nuevo nivel en el desarrollo de aplicaciones interactivas a través de Silverlight, la opción multiplataforma de Microsoft. Quien consiga dominarlo creará aplicaciones visualmente impresionantes, acordes a los tiempos de la incipiente Web 3.0.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-010-8

Flash Extremo

Este libro nos permitirá aprender a fondo Flash CS4 y ActionScript 3.0 para crear aplicaciones web y de escritorio. Una obra imperdible sobre uno de los recursos más empleados en la industria multimedia que nos permitirá estar a la vanguardia del desarrollo.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-009-2



Hackers al descubierto

Esta obra presenta un panorama de las principales técnicas y herramientas utilizadas por los hackers, y de los conceptos necesarios para entender su manera de pensar, prevenir sus ataques y estar preparados ante las amenazas más frecuentes.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-008-5

Vista avanzado

Este manual es una pieza imprescindible para convertirnos en administradores expertos de este popular sistema operativo. En sus páginas haremos un recorrido por las herramientas fundamentales para tener máximo control sobre todo lo que sucede en nuestra PC.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-007-8

¡Léalo antes Gratis!

En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.

101 Secretos de Excel

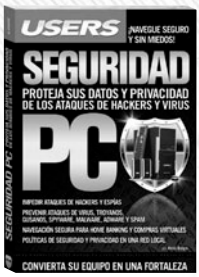
Una obra absolutamente increíble, con los mejores 101 secretos para dominar el programa más importante de Office. En sus páginas encontraremos un material sin desperdicios que nos permitirá realizar las tareas más complejas de manera sencilla.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-005-4

Electrónica & microcontroladores PIC

Una obra ideal para quienes desean aprovechar al máximo las aplicaciones prácticas de los microcontroladores PIC y entender su funcionamiento. Un material con procedimientos paso a paso y guías visuales, para crear proyectos sin límites.

→ COLECCIÓN: MANUALES USERS
→ 368 páginas / ISBN 978-987-663-002-3



Seguridad PC

Este libro contiene un material imprescindible para proteger nuestra información y privacidad. Aprenderemos cómo reconocer los síntomas de infección, las medidas de prevención a tomar, y finalmente, la manera de solucionar los problemas.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-004-7

Hardware desde cero

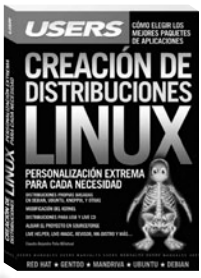
Este libro brinda las herramientas necesarias para entender de manera amena, simple y ordenada cómo funcionan el hardware y el software de la PC. Está destinado a usuarios que quieran independizarse de los especialistas necesarios para armar y actualizar un equipo.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-001-6

200 Respuestas: Photoshop

Esta obra es una guía que responde, en forma visual y práctica, a todas las preguntas que necesitamos contestar para conocer y dominar Photoshop CS3. Definiciones, consejos, claves y secretos, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: 200 RESPUESTAS
→ 320 páginas / ISBN 978-987-1347-98-8



Creación de distribuciones Linux

En este libro recorreremos todas las alternativas para crear distribuciones personalizadas: desde las más sencillas y menos customizables, hasta las más avanzadas, que nos permitirán modificar el corazón mismo del sistema, el kernel.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-1347-99-5

Métodos ágiles

Este libro presenta una alternativa competitiva a las formas tradicionales de desarrollo y los últimos avances en cuanto a la producción de software. Ideal para quienes sientan que las técnicas actuales les resultan insuficientes para alcanzar metas de tiempo y calidad.

→ COLECCIÓN: DESARROLLADORES
→ 336 páginas / ISBN 978-987-1347-97-1

SuperBlogger

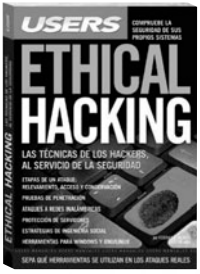
Esta obra es una guía para sumarse a la revolución de los contenidos digitales. En sus páginas, aprenderemos a crear un blog, y profundizaremos en su diseño, administración, promoción y en las diversas maneras de obtener dinero gracias a Internet.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-1347-96-4

UML

Este libro es la guía adecuada para iniciarse en el mundo del modelado. Conoceremos todos los constructores y elementos necesarios para comprender la construcción de modelos y razonarlos de manera que reflejen los comportamientos de los sistemas.

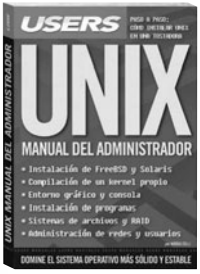
→ COLECCIÓN: DESARROLLADORES
→ 320 páginas / ISBN 978-987-1347-95-7



Ethical Hacking

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 obtener sistemas seguros y dominar las herramientas que permiten lograrlo.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1347-93-3



UNIX

Esta obra contiene un material imperdible, que nos permitirá dominar el sistema operativo más sólido, estable, confiable y seguro de la actualidad. En sus páginas encontraremos las claves para convertirnos en expertos administradores de FreeBSD.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1347-94-0

200 Respuestas: Excel

Esta obra es una guía básica que responde, en forma visual y práctica, a todas las preguntas que necesitamos conocer para dominar la versión 2007 de Microsoft Excel. Definiciones, consejos, claves y secretos, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: 200 RESPUESTAS
→ 320 páginas / ISBN 978-987-1347-91-9

¡Léalo antes Gratis!

En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.

Hardware Extremo

En esta obra aprenderemos a llevar nuestra PC al límite, aplicar técnicas de modding, solucionar fallas y problemas avanzados, fabricar dispositivos inalámbricos caseros de alto alcance, y a sacarle el máximo provecho a nuestra notebook.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1347-90-2

Servicio Técnico de PC

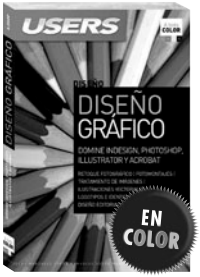
Ésta es una obra que brinda las herramientas para convertirnos en expertos en el soporte y la reparación de los componentes internos de la PC. Está orientada a quienes quieran aprender o profundizar sus conocimientos en el área.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1347-89-6

Solución de Problemas PC

En esta obra encontraremos un material sin desperdicios que nos permitirá entender los síntomas que presentan los problemas graves, solucionarlos en caso de que algún imprevisto nos sorprenda y, finalmente, evitar que se repitan.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-1347-88-9



Diseño Gráfico

Esta obra es una herramienta imprescindible para dominar las principales aplicaciones del paquete más famoso de Adobe y conocer los secretos utilizados por los expertos para diseñar de manera profesional.

→ COLECCIÓN: DISEÑO
→ 320 páginas / ISBN 978-987-1347-87-2

200 Respuestas: Redes

Esta obra es una guía básica que responde, en forma visual y práctica, a todas las preguntas que necesitamos plantearnos para conocer y dominar el mundo de las redes hogareñas, tanto cableadas como Wi-Fi.

→ COLECCIÓN: 200 RESPUESTAS
→ 320 páginas / ISBN 978-987-1347-86-5

200 Respuestas: Office

Una guía básica que responde, en forma visual y práctica, a todas las preguntas que necesitamos conocer para dominar la versión 2007 de la popular suite de Microsoft. Definiciones, consejos, claves y secretos, explicados de manera clara y didáctica.

→ COLECCIÓN: 200 RESPUESTAS
→ 320 páginas / ISBN 978-987-1347-85-8

Finanzas con Microsoft Excel

Este libro es una obra con un claro enfoque en lo práctico, plasmado en ejemplos no sólo útiles sino también reales; orientada a los profesionales que tienen la necesidad de aportar a sus empresas soluciones confiables, a muy bajo costo.

→ COLECCIÓN: PROFESSIONAL TOOLS
→ 256 páginas / ISBN 978-987-1347-84-1

Marketing en Internet

Este libro brinda las herramientas de análisis y los conocimientos necesarios para lograr un sitio con presencia sólida y alta tasa de efectividad. Una obra imprescindible para entender la manera en que los negocios se llevan a cabo en la actualidad.

→ COLECCIÓN: PROFESSIONAL TOOLS
→ 288 páginas / ISBN 978-987-1347-82-7

200 Respuestas: Hardware

Esta obra es una guía básica que responde, en forma visual y práctica, a todas las preguntas que necesitamos hacernos para dominar el hardware de la PC. Definiciones, consejos, claves y secretos de los profesionales, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: 200 RESPUESTAS
→ 320 páginas / ISBN 978-987-1347-83-4

Curso de programación PHP

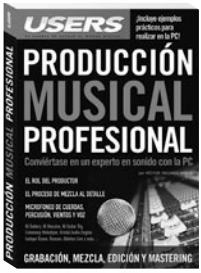
Este libro es un completo curso de programación con PHP desde cero. Ideal tanto para quienes desean migrar a este potente lenguaje, como para los que quieran aprender a programar, incluso, sin tener conocimientos previos.

→ COLECCIÓN: DESARROLLADORES
→ 368 páginas / ISBN 978-987-1347-81-0

Curso de programación C#

Este libro es un completo curso de programación con C# desde cero. Ideal tanto para quienes desean migrar a este potente lenguaje, como para quienes quieran aprender a programar, incluso, sin tener conocimientos previos.

→ COLECCIÓN: DESARROLLADORES
→ 400 páginas / ISBN 978-987-1347-76-6



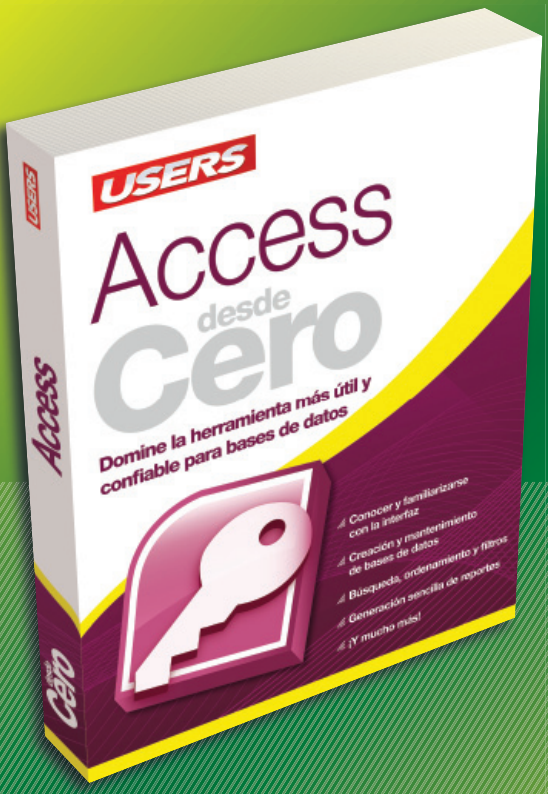
Producción musical profesional

Esta obra es un manual preciso y detallado que permite alcanzar la perfección a quienes quieren lograr el sonido ideal para sus composiciones. Está enfocado en el rol del productor, lugar desde donde construye los cimientos para producciones profesionales.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-1347-75-9

DOMINE LA HERRAMIENTA MÁS ÚTIL Y CONFIABLE PARA BASES DE DATOS

Access es el programa por excelencia para bases de datos a nivel hogareño y, además, el más utilizado a nivel mundial. Esta obra es ideal para entender cómo crear y administrar datos en un nivel complejo con la aplicación de bases de datos de Microsoft.



» HOME / WINDOWS
» 192 PÁGINAS
» ISBN 978-987-1773-11-4

SOBRE LA COLECCIÓN desde Cero

- Aprendizaje práctico, divertido, rápido y sencillo.
- Lenguaje simple y llano para una comprensión garantizada.
- Consejos de los expertos para evitar problemas comunes.
- Guías visuales y procedimientos paso a paso.

OTROS TÍTULOS DE LA MISMA COLECCIÓN

PHOTOSHOP // OFFICE // HARD
WINDOWS 7 // BLOGS // REDES
SEGURIDAD // Y MUCHO MÁS

LLEGAMOS A TODO EL MUNDO VÍA OCA* Y DHL**

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

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

Hacking desde Cero

En la actualidad, los ataques informáticos están a la orden del día. En esta obra, enseñamos todas las posibilidades de ataque a las que estamos expuestos en todo momento, así como también los métodos para proteger nuestra información ¡y para no caer víctimas de los hackers!

Dentro del libro encontrará

Seguridad en la información | Defensa en profundidad | Espionaje corporativo | Delitos informáticos | La evidencia digital | Metodología de investigación | Ethical Hacking | Tipos de ataque | Seguridad física y biométrica | Acceso a las instalaciones | Personal de seguridad | El mundo web | Autenticación web | Recopilación de información | Ataque de inyección | Sniffing / Spoofing | Hijacking | Honeypots | Marco legal | Pentration testing | Metodología de análisis

Sobre la colección

- Aprendizaje práctico, divertido, rápido y sencillo
- Lenguaje simple y llano para una comprensión garantizada
- Consejos de los expertos para evitar problemas comunes
- Guías visuales y procedimientos paso a paso

Otros títulos de esta misma colección

Soluciones PC / Seguridad PC / Secretos Excel / Blogs / Proyectos Windows / Técnico Hardware / Redes

Hacking from scratch

Today, cyber attacks are on the agenda. This book prevents us from all kinds of attacks to which we are exposed throughout time, as well as the methodologies to protect our information and to avoid being victims of hackers!

RedUSERS.com

Nuestro sitio reúne a la mayor comunidad de tecnología en América Latina. Aquí podrá comunicarse con lectores, editores y autores, y acceder a noticias, foros y blogs constantemente actualizados.

Si desea más información sobre el libro:
Servicio de atención al lector **usershop@redusers.com**

El contenido de esta obra formó parte del libro *Hackers al descubierto* y *Ethical Hacking*.

ISBN 978-987-1773-03-9