1 > El hacking ético.

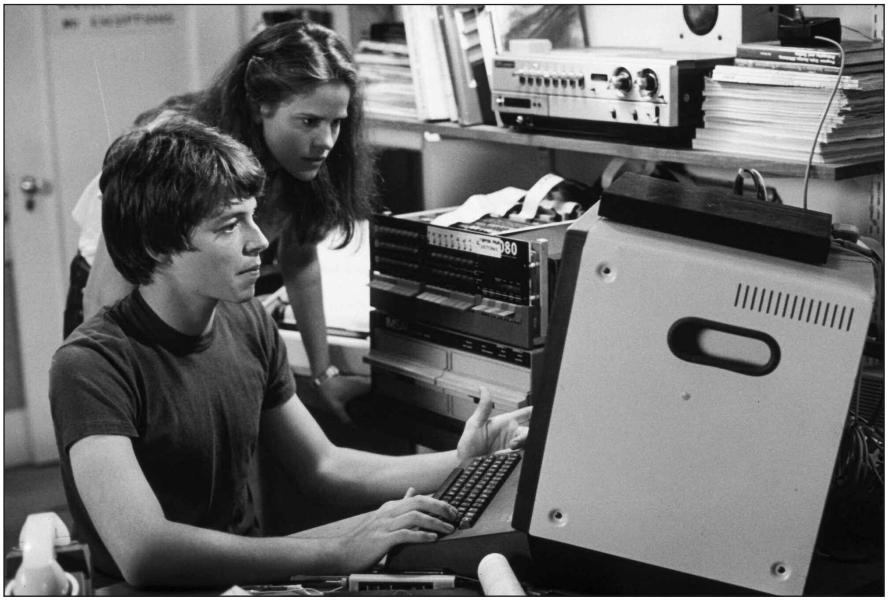
Referencias históricas de sucesos y de evolución en la materia. Cómo se comenzó a implementar el hacking ético, por quiénes y sus características; en dónde y de qué modo actúan o se forman estos profesionales. También conoceremos material sobre aspectos importantes de las organizaciones y las definiciones básicas de los componentes involucrados.

UN POCO DE HISTORIA

Si tu intención es describir la verdad, hazlo con sencillez y la elegancia déjasela al sastre.

Albert Einstein.

Hace algún tiempo, cuando algunas de las organizaciones apenas comenzaban a incrementar los procesos informatizados dentro de su sistema de información, sus propios administradores y analistas técnicos eran los encargados de buscar claras falencias o brechas de seguridad en el escenario para solucionarlas como podían. En ese entonces, la mayoría no tenía una noción madura acerca de la seguridad de la información o de las intrusiones de terceros no autorizados en sus sistemas. A medida que pasó el tiempo, estas organizaciones se multiplicaron de manera notable y se informatizaron aún más, incluso tomando a Internet como plataforma de sus movimientos de información. De ese modo, se hicieron fluidas las **comunicaciones interpersonales**, **intersucursales**, transacciones o **flujo digital** de todo tipo y nivel de importancia, dejando, al mismo tiempo, muchos más datos expuestos a terceros, como nunca antes había sucedido.



Hackers. Matthew Broderick y su compañera de reparto en War Games (1983). El público en general conoce así a los hackers.

Como resultado de ello y debido a que grandes casos de intrusión se dieron a conocer al público en general a través de los medios de prensa (aunque muchos no

salen a la luz para salvaguardar una imagen institucional de organización confiable), se hizo evidente la falta de algún servicio profesional que imitara esos ataques o capacitara a su personal con las mismas metodologías que utilizaba el intruso. De esa manera, se podían evaluar las reales condiciones de seguridad en las que se encontraba una organización y, de existir agujeros en el sistema o potenciales brechas, descubrirlos y solucionarlos de forma preventiva.

Chacal. Actualmente, Kevin Mitnick es un empresario relacionado a la seguridad de la información y autor de dos interesantes libros.

Los accesos no autorizados, junto a una gama de vulnerabilidades y todo tipo de amenazas relacionadas o dirigidas hacia la información, estaban a la orden del día. Desde algunos años antes, muchos especialistas ligados a la seguridad informática venían estudiando y practicando metodologías de intrusión en sus trabajos, laboratorios o casas. Así, comenzaron a brindar a las organizaciones un servicio a modo de proveedores externos o contratados y, para darle un nombre medianamente formal, lo llamaron **ethical hacking**. Este concepto incluye las denominaciones **vulnerability scanning** y **penetration test**, mejor denominado **network security assessment**.

Había una clara demanda de seguridad y, donde existe demanda, aparece una oferta. Por lo tanto, allí mismo nace un mercado. Apenas mediaban los años 90, ya asomaban las épocas de **e-commerce**, comenzaba la integración de las pequeñas y medianas empresas de todo el mundo a la red (e-organizaciones), a la que poco a poco se sumaba el público en general. Aparecía **malware** más sofisticado, se publicaban novedosas técnicas de intrusión o explotación de vulnerabilidades y no había demasiada conciencia sobre la administración segura de los servidores.

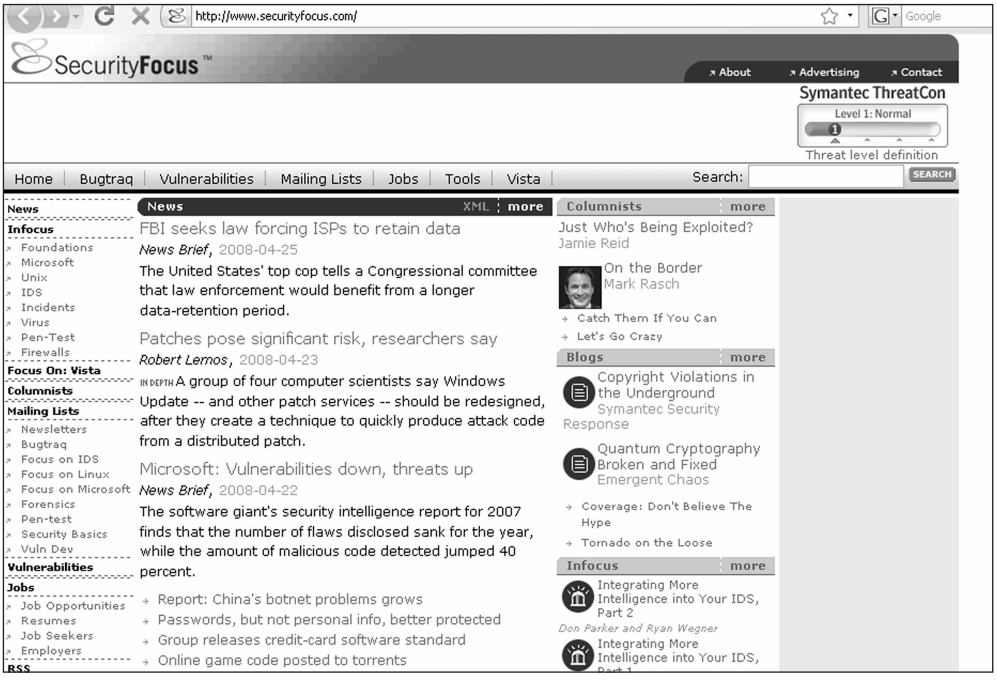
Al mismo tiempo, jóvenes de todo el mundo se colaban en Internet engañando las

Malware

Con este nombre, se conoce todo aquello que se cataloga como código malicioso (programas). Generalmente, estas amenazas son detectadas por los antivirus, se trate de gusanos o worms, spyware, troyanos, virus o scripts malintencionados (en rutina de tiempo o de ejecución).

centrales telefónicas (por una cuestión de gastos) de sus países para divertirse con los sistemas informáticos e intercambiar conocimientos con sus pares del otro lado del globo. De ese grupo de gente, saldría lo que en esos días serían algunos de los mejores profesionales de la seguridad, así como también ***hábiles intrusos.***

Este fenómeno pudo ser posible gracias a la ausencia de una plataforma educativa formal sobre el tema, ya que los recursos de aprendizaje eran, y a menudo son (hoy más que nunca), compartidos. En aquel entonces, sobre seguridad no había educación formal más allá de un postgrado en alguna universidad de EE.UU. o la que ofreciera una institución privada para sus empleados. En un ámbito más informal, recién en el año 1993, nació **Bugtraq**, una conocida lista de correo en la que se tratan temas de seguridad. No fue todo de un día para el otro, pero tuvo una marcada evolución.



Securityfocus. La mejor definición de Bugtraq (actualmente alojada en www.securityfocus.com) se encuentra en Wikipedia, ya que incluye su historia completa.

Exploit

O xploit, es un programa de prueba de concepto que puede estar en código fuente para compilar (fuente.c) o formato binario tipo .exe. Sirve para aprovechar o demostrar una vulnerabilidad en una aplicación y puede estar escrita en varios lenguajes de programación. En securityvulns.com/exploits, encontramos un repositorio de Proof of concept.

AÑO	SUCESO
1982	John Shoch (uno de los creadores de ethernet), junto a un colega, escribieron el primer reporte sobre un gusano (worm), tomando ese nombre de una novela de ciencia ficción de 1975 en la que, bajo el nombre Tapeworms, describían a programas autómatas que viajaban por las redes transportando información.
1983	Ese año se estrenó la famosa película War Games, en la que el actor Matthew Broderick interpretaba a un chico que ingresaba en una base militar a través de su computadora y casi desata una guerra nuclear.
1984	Se crearon la publicación 2600, el CCC chaos computer club, Legion of doom y la división de fraude con tarjetas y computadoras del Servicio Secreto.
1988	Robert Tappan Morris soltó un gusano en Arpanet (como se llamaba Internet antes) y de ese modo infectó miles de servidores Unix. Fue enjuiciado y conde nado a cumplir 400 horas de trabajo social.
1992	Kevin Mitnick, luego de estar prófugo y ser atrapado por el FBI, fue sentenciado por robo de software e intrusiones en organizaciones.
1994	Vladimir Levin robó, desde San Petersburgo, a través de los sistemas de Citi bank, más de 10 millones de dólares por medio de transferencias a sus cuentas. En los dos años siguientes, desde otros bancos de los Estados Unidos, 300 mi llones de dólares se movilizaban electrónicamente de modo fraudulento.

Sucesos. Algunos hechos importantes de la historia del hacking.

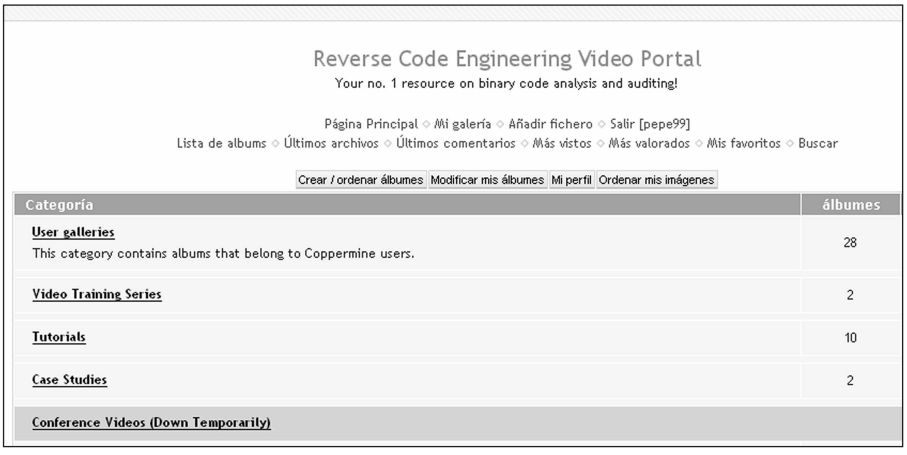
¿POR QUÉ ÉTICO?

Para **emular la metodología** de ataque de un intruso informático y no serlo, tiene que haber **ética** de por medio, más allá de todas las condiciones, términos y activos que haya alrededor del caso. Imaginemos que las autoridades de un banco contratan a alguien para que simule un robo (no a mano armada, claro está) y de ese modo se pruebe la eficiencia de su sistema de seguridad. Este supuesto ladrón profesional, luego de lograr su cometido, informa a sus dueños en detalle cómo pudo hacerlo y cómo ellos deberían mejorar su sistema de seguridad para que no volviera a pasar. Lógicamente, no se puede encargar de hacer esto una persona sin ética, alguien inmoral. No entraremos en el terreno de lo ético como rama dentro de la filosofía práctica ni redactaremos un tratado sobre deontología profesional, no sólo por la cuestión de espacio, sino también por respeto a los griegos. Sí, en cambio, diremos que la ética implica que el trabajo y la intervención del profesional en seguridad informática o de la información no comprometen de ningún modo los activos de la organización, que son los valiosos datos con los que ella cuenta.

Estos daños podrían ser hechos de varias maneras: **alteración**, modificando a conciencia registros o datos sensibles; **borrado**, destruyendo información, bases de datos o sobrescribiendo algún tipo de dato; **dar a conocer información a terceros**, incumpliendo las normas de confidencialidad; **sustracción**, robando o guardando datos en medios de almacenamiento externos. Todo esto, ya sea en la búsqueda de riesgos mediante un **security assessment** o comprobación de seguridad, como también en la divulgación de lo que se vio, habló, escuchó o manipuló en el transcurso, en la planificación o en el desarrollo de la tarea misma y en su análisis final. Más allá de la ética propia de cada profesional, existen conductas mínimas que éste debe cumplir:

- Hacer su trabajo de la mejor manera posible.
- Dar el mejor reporte.
- Acordar un precio justo.
- Respetar el secreto.
- No hablar mal ni inculpar a un administrador o equipo de programadores.
- No aceptar sobornos.
- No manipular o alterar resultados o análisis.
- Delegar tareas específicas en alguien más capacitado.
- No prometer algo imposible de cumplir.
- Ser responsable en su rol y función.
- Manejar los recursos de modo eficiente.

En nuestros tiempos, para la mayoría de la gente y de la prensa, la palabra hacking está ligada a delincuentes comunes, a personas de dudosa moralidad que utilizan conocimientos de informática o electrónica para delinquir. Por tal motivo, en el transcurso de este libro, sólo citaremos como personajes a dos figuras: al **profesional ético** y a su opuesto, el **intruso**, para que no haya malentendidos de ningún tipo.



Inversa. Portal sobre ingenieria inversa: video.reverse-engineering.net

Ejemplo de ethical hacking

Para comprender mejor el concepto de hacking ético, analicemos un caso. ¿Es ético ingresar en una casilla de correo electrónico ajena sin conocer su password? Bajo las posibilidades que brinda el **ethical hacking**, por supuesto. Esa situación puede darse siempre y cuando la casilla de e-mail sea de alguien que nos haya autorizado, como profesional ético, a demostrarle que su organización es vulnerable. Como una casilla es personal (quizás de un gerente o de un administrador de sistemas), posiblemente ese ingreso nos lleve a obtener acceso a determinado lugar o a datos sensibles. Éstos, a su vez, serán utilizados para lograr entrar en un servidor y de allí dirigirnos hacia la red interna, con todo el riesgo que significa para una organización formal altamente informatizada. De ese modo, descubriremos pequeños descuidos que, desde un lugar impensado, pueden exponer a la empresa por completo. Sin embargo, esta vez, ese riesgo pasaría rápido a la historia, ya que estamos hablando de un típico caso de **ethical hacking**, en donde el problema es intensamente buscado, descubierto, analizado, reportado y por último solucionado a la brevedad.

Para lograr algo así, se requieren dos elementos básicos: en principio, **metodología** para proceder. Esto es el resultado de un grupo de piezas previamente ensambladas: habilidades personales de lógica y creatividad, técnicas propias de un **network security assessment**, reconocimiento o relevamiento de todos los componentes del escenario y herramientas como un intérprete de comandos del tipo **prompt** o **shell**, un web browser y un editor de texto, al menos para este caso.

Por otro lado, se requiere **autorización**, que es el elemento más importante. Esta autorización también tiene sus partes: un **contrato de confidencialidad**, coordinación, evaluación, procesos por seguir y todas las características internas (por ejemplo, el compromiso de la gerencia para con el proyecto es vital) o propias de las partes involucradas en este trabajo/desafío.

Para resumir, veamos el proceso de ethical hacking en pocas palabras:

1. La organización desea saber si sus sistemas son realmente seguros.

Lectura sobre ética

Es muy interesante el texto Ética empresarial, teoría y casos, del autor Rafael Gómez Pérez. Y para conocer más sobre el aspecto ético del hacking ligado a la seguridad de la información, es recomendable el libro La ética del hacker y el espíritu de la era de la información, del autor Pekka Himanen, con prólogo de Linus Torvalds.

2. Selecciona y contrata un servicio profesional de ethical hacking.
3. Lo autoriza a realizar el trabajo mediante diversas pautas.
4. Planifican estratégicamente cómo se realizará y el alcance que tendrá.
5. El profesional, luego de llevar a cabo los análisis preliminares, realiza su tarea imitando al atacante real, pero sin comprometer dato alguno.
6. Luego, analiza los resultados del security assessment.
7. Confecciona un reporte detallado para que la organización lo evalúe.
8. Soluciona lo vulnerable o mitiga lo potencial para dejar el sistema más seguro. Se reafirma la defensa del sistema en general.
9. Se adoptan políticas de control y seguimiento (normativa).

> *Ethical hacking es una metodología utilizada para simular un ataque malicioso sin causar daño.*
>
> **E-council – CEH v5.0**

Formación del Profesional

Knowledge is power.

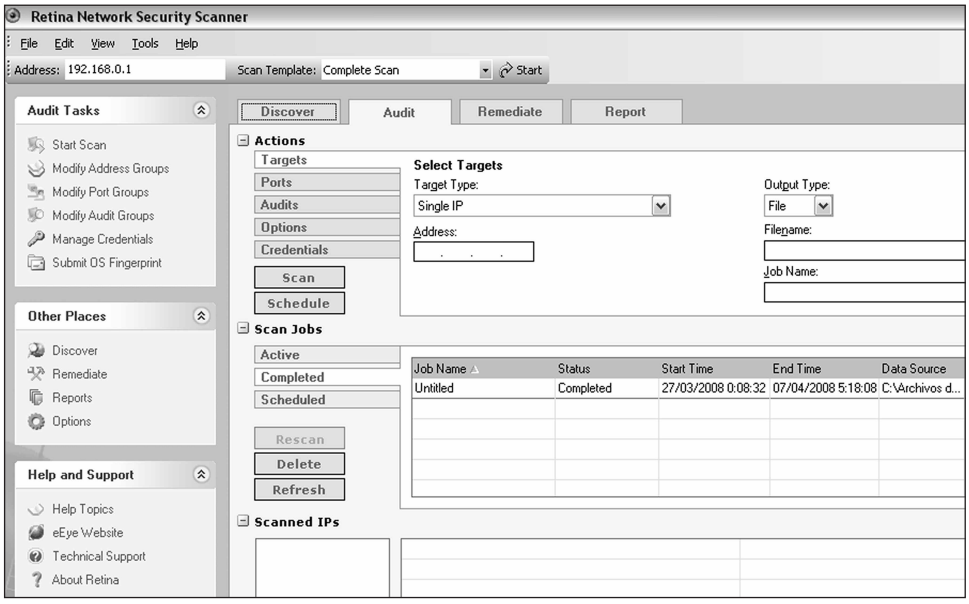
Sir Francis Bacon.

Una anécdota conocida (que data de la época de las **BBS**, Bulletin Board System, allá por los años 90) describía cómo dos jóvenes ingresaron en los sistemas de un laboratorio espacial. Éstos lo lograron luego de haber intentado muchas contraseñas entre las cuales había nombres de constelaciones, cometas y planetas. Finalmente, acertaron con un usuario de sistema que tenía, como clave, el nombre de una lejana estrella. El profesional de seguridad, al llevar a cabo un network security assessment como parte de su trabajo de ethical hacking, necesita contar con ese tipo de lógica y tiene que aplicarla, más allá de utilizar las técnicas y herramientas (open source, comerciales o privadas), dado que necesita imitar un ataque de la mejor manera y con el máximo nivel posible. Para eso, tendrá que emplear todos los recursos de **inteligencia** que tenga a su alcance, utilizar al extremo sus **conocimientos**, poder de **deducción** y **análisis** mediante el **razonamiento** y así determinar qué es lo mejor que puede intentar, cómo, dónde y con qué. Por ejemplo, saber si un pequeño dato, por más chico o insignificante que parezca, le será útil y cómo proseguir gracias a él.
Continuamente deberá enfrentarse a etapas que le demanden la mayoría de estas aptitudes:

- Saber cómo definir patrones de conducta y acción.
- Hacer relevamientos pasivos de información.
- Interpretar y generar código, cifrado y entropías de datos.

- Descubrir manualmente descuidos en el objetivo.
- Descubrir vulnerabilidades presentes de todo el escenario técnico.
- Buscar lógica e ilógicamente.
- Proyectarse sobre la marcha en modo abstracto, táctica y estratégicamente.
- Ser exhaustivo, pero a la vez saber cuándo es el momento de recurrir a la distensión (para no agotar la mente).
- Ser ético por sobre todas las cosas.

Si estas condiciones personales y culturales del profesional no son las adecuadas (por tener poco ingenio, poca cultura general o imaginación que impida ejecutarlas), éste no será eficiente en su trabajo. No tendrá el valor agregado de quien va más allá de las metodologías que se pueden interpretar siguiendo un simple checklist o un determinado **manual de procedimiento**.
Una carencia en alguno de estos aspectos podría significar el no descubrir una brecha potencial de seguridad apenas perceptible presente en el sistema o que, a futuro, un atacante real más inteligente y experimentado sí lo haga.
Nadie dijo que esto era fácil. Para hacer un chequeo de seguridad en un entorno, no basta con sólo colocar a trabajar un **scanner** (buscador) de vulnerabilidades sobre una dirección IP y sentarnos a esperar su resultado.



Retina. Pantalla del buscador de vulnerabilidades Retina, de la empresa Eeye .

Un colega, de nombre Clement Dupuis, luego de discutir uno de los aspectos de la educación sobre seguridad en la lista Bugtraq, hizo el siguiente comentario: **Nece-**

sitamos gente técnica, necesitamos gente que mire todo el escenario, necesitamos gente con habilidades sociales, necesitamos gente sin habilidades sociales, pero con mucha lógica. Esto da una pequeña idea acerca de los perfiles y características que se necesitan tanto para la parte técnica como para la gestión, la comunicación y la resolución de problemas lógicos. Llegar a ser un profesional muy bueno, que pueda manejarse cómodamente en todos o en gran parte de los perfiles, puede requerir varios años de estudio, práctica y trabajo. Son tantas las variables y componentes tecnológicos involucrados (además de la necesidad de mantenerse constantemente informados), que es imposible conocerlos, entenderlos y aplicarlos de un modo eficiente de un día para otro.

OSI. Es importante conocer protocolos de comunicación. En este caso, el modelo OSI.

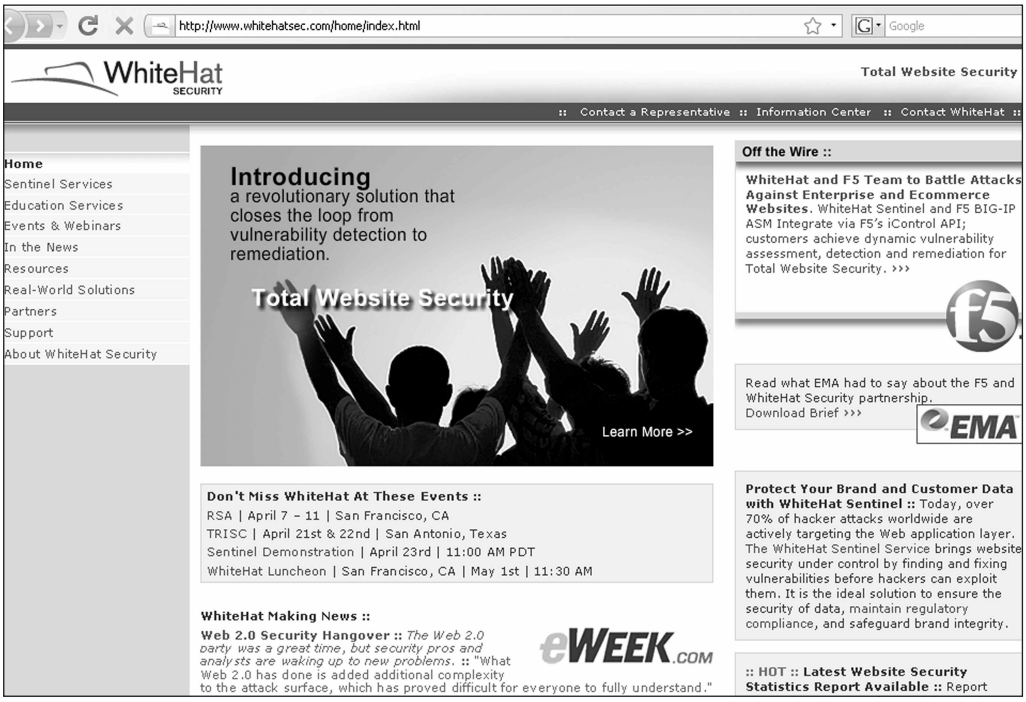
Los componentes que aparecen a continuación son una gran parte del aspecto técnico que hay que conocer y estudiar, sin tener en cuenta todo aquello que comprende el manejo de políticas y normativas en el aspecto seguridad y organización (gestión), sumado a las cuestiones de origen personal o la capacidad de llevar adelante grupos y proyectos. Idiomas, sistemas operativos, **hardware**, malware, comandos, **networking** y **topologías**, **auditorías**, lenguajes de **programación**, **cifrados**, **análisis** de resultados, conectores, vulnerabilidades, herramientas, técnicas de **intru-**

sión, IDS, databases, diseño lógico, aplicaciones, relevamientos y **protocolos** de comunicación (familia TCP/IP entre otros).
El material es tan vasto que podría alienar a un ser humano si este no lo asimilara con cautela, y por ello es muy importante no lidiar con material inútil y tener bien presentes las fuentes correctas de estudio o práctica. Tratar de ver a la vez un poco de todo es una pérdida de tiempo, que es lo más valioso que tenemos. Por ese motivo, hay que darse cuenta y tratar de descubrir las aptitudes y habilidades (**skills**) de cada uno, cultivarse de forma adecuada y practicar o trabajar en base a ello.
La formación puede orientarse a medida que el profesional o estudiante decida hacia qué lado desea inclinarse en la materia, ya que no es lo mismo ser un desarrollador de **exploits** en C++ que redactar políticas de acceso físico en recintos o configurar, de modo seguro, un servidor Linux.
Si bien no se puede ser un experto en todo, lo más recomendable es que, luego de dominar bien un perfil, se comience a estudiar los componentes de otro. Sumado a eso, hay que mantenerse bien informado sobre las vulnerabilidades actuales, las metodologías, los recursos de aseguramiento y las medidas de prevención.

Santiago Cavanna, profesional de la seguridad de la información, me hizo el siguiente comentario: "a veces es conveniente tambien cultivar el trabajo colaborativo entre varios especialistas, de esa manera, se cultiva la especialidad en profundidad y luego se desarrolla un tipo de conocimiento que permite integrarse en un equipo de trabajo." tambien citó del libro "El arte de resolver Problemas" (isbn:968-18-1294-8) "El que tiene que tomar una decisión trata de elegir un curso de acción que produzca el resultado deseado, uno de que sea eficaz respecto a lo que el valora. Estos cursos de acción se conocen como efectivos. La efectividad es producto de la eficiencia y el valor. El que busca el mejor y más efectivo curso de acción se dice que optimiza.
El que busca una solución que sea suficientemente buena, se dice que satisface."

Eficaz o eficiente

La diferencia entre ser **eficaz** y **eficiente** consiste en que el primero sólo cumple con el objetivo, mientras que el segundo no sólo lo cumple, sino que lo hace generando el menor gasto de recursos (ya sea tiempo, dinero, herramientas o personal involucrado).



Whitehat. En www.whitehatsec.com hay documentos en inglés acerca de vulnerabilidades y técnicas muy interesantes.

RECURSOS PARA EL ESTUDIO

Los motivos por los que alguien puede llegar a dedicarse al ethical hacking son variados, y algunos géneros pueden destacarse más que otros. Por un lado, podemos mencionar aquellos que la ven como una interesante rama de la informática de nuestros tiempos, o que necesitan conocerla porque su posición en el trabajo así se los demanda. También existen quienes llegaron hasta aquí por su pasión temprana o más reciente, hacia los sistemas como hobbie. Tampoco faltan quienes vieron alguna película y se fascinaron con los personajes del tipo hacker llamados **Zero Cool** o **Acid Burn**. Por último, existen aquellos que desean generar y obtener ga-

Cursos de inglés

Si queremos aprender inglés de forma no presencial u obtener certificaciones internacionales, podemos visitar sitios como RosettaStone (www.rosettastone.com), Pimsleur (www.pimsleurapproach.com), University of Cambridge (www.cambridgeesol.org), IELTS (www. ielts.org), EuroTalk (www.eurotalk.co.uk) y Bulats (www.bulats.org).

nancias comercializando productos o servicios relacionados con la materia.
Lógicamente, no todos los que ingresan en el tema lo transitan con la misma formación, ya sea académica, formal o autodidacta, salvo en la etapa básica de educación. Quizá sea éste el único punto en el que pueden alcanzar cierto grado de similitud o equilibrio en la preparación. En cuanto al resto de las etapas, esa preparación es demasiado difusa por el problema de modelo educacional. Por tal motivo, la formación sobre el tema está más ligada al aspecto **autodidacta** y de experiencia que a un modelo de carrera focalizado y especialmente diseñado. Los recursos de formación recomendados que veremos en este capítulo están divididos en cuatro etapas fundamentales:

- Formación básica.
- Educación autodidacta.
- Educación formal.
- Trabajo & práctica: experiencia.

Formación básica

Es muy probable que la mayoría de los lectores de este libro hayan pasado por esta etapa junto a educadores, padres o tutores. Esta etapa inicial es la base de una temprana educación. Por más absurdo que parezca, este tipo de formación intelectual básica tiene clara incidencia en el desempeño de un profesional de sistemas, más allá de la especialidad que éste elija cuando sea adulto. En esta etapa podemos mencionar:

- La familia y el colegio como primeros contactos con la informática formal e informal. Estímulos, ambiente, introducción en las matemáticas.
- El estudio de idiomas como el **inglés**, fundamental en informática para la interpretación de manuales y la comunicación en listas de correo.
- Años tempranos en los que se alienta a socializar, jugar en equipos, participar de actos y hacer amistades.
- Jugar al **ajedrez** como desarrollo de la lógica estratégica y táctica.
- Juegos de **ingenio** como estímulo de capacidades analíticas y resolución de proble-

Juegos de ingenio

Internet es una fuente inagotable de recursos. Si queremos mejorar nuestra capacidad e ingenio mediante juegos, podemos ingresar en sitios como www.mlevitus.com, www.juegosdeingenio.org, www.pumbo.com/index.php?g=2 y www.mensa.es/juegosmensa/juegos.html.

mas.

- Incentivo del hábito de la **lectura**, que dará cierta facilidad para redactar y comunicarse mejor con diferentes tipos de personas, y ayudará al desarrollo de la **creatividad** y de la **imaginación**.
- Por último, algo muy importante: conocer lo **moralmente correcto**.

Ajedrez. En el sitio www.ajedrez21.com, encontramos recursos dedicados al aprendizaje del ajedrez.

Educación autodidacta

Ser **autodidacta** significa estudiar por cuenta propia. Permite la elección propia y es la que más perfilará al futuro profesional de seguridad, ya que se comienza estudian-

Hola mundo

El ¡Hola mundo! es conocido por ser lo primero que se intenta en cualquier lenguaje de programación. Esta práctica consiste en imprimir esas dos palabras en la pantalla cuando es ejecutado el pequeño programa que se desarrolla. Podemos encontrar más información y ejemplos en http://es.wikipedia.org/wiki/Hola_mundo.

do por gusto, afinidad y libre elección del material. Para ser un buen profesional en seguridad informática o de la información, conviene aprender este tipo de cosas:

- Aprender a **programar** y **analizar** problemas lógicamente.
- **Administrar** sistemas operativos diferentes y **configurarlos**.
- Aprender acerca de networking y protocolos de comunicación.
- Conocer seguridad informática y de la información, principalmente las técnicas más usuales de intrusión y los métodos de gestión.

¿Cómo se aprende a programar? Simplemente programando. Ya sea desde cero (con el famoso **¡Hola mundo!**) o mirando código fuente ajeno y tratando de interpretar qué fue lo que intentó hacer el autor, pensar cómo podría haberlo hecho mejor y luego optimizarlo. Estas premisas son válidas bajo cualquier idioma de programación, que no son más que **comandos**, determinada **sintaxis** (forma de escribirlo) y **lógica** para la resolución del problema. Aunque requiere dedicación, puede programar quien se lo proponga y haga el sacrificio. La diferencia en calidad la dará el esfuerzo y la lógica creativa de cada uno, que nos llevará a hacer lo mismo en diez o en mil líneas de código, o bien en diez o en mil horas de trabajo.
Programar o saber **interpretar código fuente** será de gran utilidad para muchas cosas relacionadas con la seguridad informática. Nos ayudará a solucionar problemas dentro de un sistema (con programación **bash**, **scripting** y **WSH** en entornos Linux o Windows), a construir, o modificar, pruebas de concepto de cualquier tipo y arquitectura o lenguaje. También nos servirá para realizar administración avanzada mediante scripts, hacer y modificar herramientas o aplicaciones y auditar código propio o ajeno. Por otro lado, nos permitirá **migrar código** de un idioma a otro, modificar open source (código fuente de sistemas Linux por ejemplo), hacer **ingeniería inversa** de parches, malware o aplicaciones y depurar, entre otras cosas. Con estos conocimientos, también podremos **testear** aplicaciones online o en red de forma local, **optimizar** todo tipo de código, **automatizar** secuencias de comandos, hacer reportes, monitoreos, flujo de datos o accesos y proteger código mediante el empaquetamiento de binarios, por ejemplo. Como vemos, las posibilidades son muchas.

Diagramación sin PC

Si deseamos crear diagramas de forma manual, en las librerías podemos conseguir diversas plantillas para esto según la norma IRAM 36002. Al estilo de los stencils, estas plantillas plásticas tienen diferentes utilidades y aplicaciones, como podemos ver en www.plantec.com.ar/local-cgi/vercategoria.cgi?codigo=9.

No es necesario aprender todos los lenguajes, ya que son decenas y podría llevarnos muchos años sin que alcancemos a darles una real aplicación. Es muy importante que un buen programador, una vez experimentado, programe de modo seguro.
Una temprana y buena práctica, que hoy no se acostumbra a estudiar, es la **diagramación lógica**, válida también para iniciarse en algunos lenguajes de programación (del tipo batch) ya que facilita el desarrollo de la **lógica secuencial**.

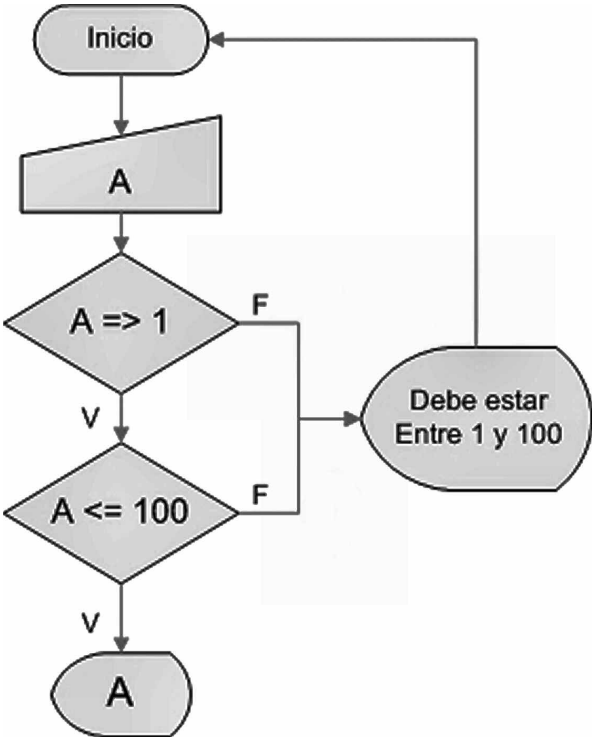


Diagrama. En este diagrama hecho a mano, que se tienen que mostrar en pantalla números entre 1 y 100. Condición falsa (F), condición verdadera (V). El gráfico de rombo equivale a un IF o decisión.

Listas de correo

De la misma manera que en los foros, pero mediante correos electrónicos, podemos obtener ayuda en las listas de correo. Para encontrar estas, ingresamos en sitios como www.egrupos.net, http://groups.google.es, http://es.groups.yahoo.com o http://groups.blogdigger.com y utilizamos palabras clave relacionadas con el tema.

Para ayudarnos con nuestro aprendizaje, podemos recurrir a Internet, tanto a sitios como a foros y listas de correo. Por ejemplo, **Psicofxp.com** es la mayor comunidad online en español y cuenta con excelentes foros dedicados a tecnología. Tanto en programación (**www.psicofxp.com/forums/programacion.313**) como en otras áreas IT, este sitio cuenta con gente dispuesta a ayudarnos de manera desinteresada. Recurrir a foros de programadores es una muy buena alternativa, en especial cuando recién comenzamos a programar de modo autodidacta, ya que podemos publicar nuestra consulta y esperar a que programadores más experimentados nos respondan o guíen hasta la solución.

Psicofxp. En www.psicofxp.com, podemos encontrar mucha ayuda cuando comenzamos a programar.

Además, en Internet podemos encontrar repositorios de código y tutoriales de todos los lenguajes existentes. Veamos algunos sitios.

FreeBSD, NetBSD y OpenBSD

Si queremos aprender más sobre los sistemas operativos FreeBSD, NetBSD y OpenBSD, podemos visitar las siguientes direcciones: www.undeadly.org, www.eldemonio.org, www.freebsd.org.mx y www.bsdfreak.org. En estos sitios, encontraremos tutoriales, novedades e información complementaria que nos será de utilidad.

LENGUAJE	URL
Planet Source Code	www.planet-source-code.com
Linux Scripting	www.freeos.com/guides/lsst
Programación Bash	xinfo.sourceforge.net/documentos/bash-scripting/bash-script-2.0.html
Win32 Scripting	http://cwashington.netreach.net
Assembly	www.csn.ul.ie/~darkstar/assembler/manual
Python	www.python.com.ar
C	www.cti.uib.es/MESINFO/MANUALS/CursC.pdf
C++	www.conclase.net/c
Perl	http://perlenespanol.baboonsoftware.com
Visual Basic	www.vb-mundo.com
PHP	www.php.net
ASP	www.soloasp.com.ar
Javascript	www.gamarod.com.ar

Programación. Sitios en los que podemos encontrar material sobre distintos lenguajes de programación.

Aprender acerca de los sistemas operativos

Los grandes escenarios suelen estar compuestos por diferentes componentes o servidores bajo plataformas como Unix, Solaris, Linux, FreeBSD, OpenBSD o Windows Server. Por lo tanto, no es recomendable dedicarse sólo a conocer y administrar una plataforma única si estamos decididos a abordar la seguridad informática en cuestiones técnicas (a menos que deseemos especializarnos y delegar el resto del trabajo) o bien formar parte de un equipo.

Los chequeos de seguridad se pueden llevar a cabo desde diferentes sistemas operativos ya que no todos ofrecen las mismas condiciones de trabajo, versatilidad y herramientas. Para mejorar nuestros conocimientos, un buen comienzo es aprender a administrar estos sistemas operativos, conocer cómo funcionan, su configuración segura y de red, su estructura interna, los comandos usuales y los avanzados, los controles que tiene, sus logs o archivos de auditoría, cómo instalar aplicaciones en él y también setearlas, cómo actualizarlo, parchearlo o modificarlo, y ver la estructura y las limitaciones en los privilegios de cada grupo de usuarios. Lógicamente, para aprender a administrar un servidor, ya sea Unix, Linux o Windows, primero hay que instalarlo. Luego se deben utilizar sus comandos y estudiar su estructura interna, gestionar los usuarios del sistema y sus diferentes permisos, conocer cada servicio nativo y deshabilitar aquellos que sean innecesarios, crear relaciones de confianza entre otros componentes en red a través de diversos métodos. También, auditar sus archivos de registro, conocer bien los logs y cuál es la in-

formación relevante que se deposita en ellos, intentar el filtrado de protocolos y conexiones externas, mantener actualizado todo lo posible (incluido el kernel en el caso de Linux), determinar qué cosas no pueden dejarse por defecto (como passwords, usuarios, aplicaciones, paths o directorios, privilegios, configuraciones o archivos), probar aplicaciones y tecnologías usuales como apache, mysql u openssl.
De ese modo, se comienzan a aplicar los métodos de **hardening**, que significa **volver más seguro** el servidor, y se van adquiriendo nociones de administración avanzada. A su vez, esto nos ayuda a conocer las características débiles de un sistema instalado por default, lo que nos permitirá reconocerlas fácilmente en los futuros escenarios en los que estemos involucrados.
La instalación y la administración seguras de servidores llevada a cabo de un modo realmente eficiente, ayudará a prevenir la intromisión en el sistema (a través del sistema operativo) de alguien no autorizado. De todos modos, un sistema operativo es apenas una puerta entre la decena de posibilidades.

BSD. En www.bsdargentina.com.ar, encontraremos foros y diverso material acerca de la familia BSD.

Ante alguna duda puntual relacionada con los sistemas operativos, debemos recordar que en Internet se encuentran listas de correo de usuarios, mailings oficiales de los desarrolladores, mailings de empresas con productos afines (por ejemplo eEye), foros de discusión, canales IRC, blogs, FTP, cursos, libros, e-zines, monografías, grupos de usuarios, asociaciones, desarrolladores, depósitos de aplicaciones y código fuente.

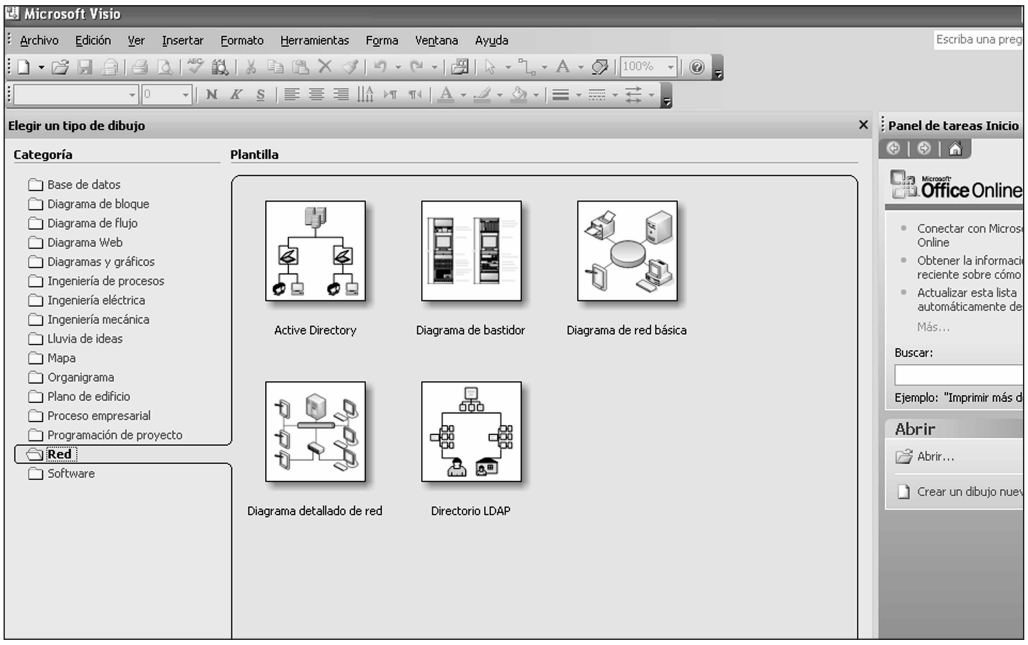
Aprender acerca de networking

El conocimiento de networking y todo aquello referente a redes (como protocolos y conectores, routing y switching, entre otras cosas) es básico para el diseño y la diagramación de entornos de una organización, pero resulta fundamental para un futuro profesional de ethical hacking.

RFC. Los RFC (Request For Comments) son los estándares que definen cada uno de los componentes de Internet. Consisten en la lectura básica y muy detallada de los protocolos utilizados. Los podemos ver en español en www.rfc-es.org.

Esto nos permitirá no sólo llevar a cabo el chequeo de seguridad e interpretar el mapeo de los componentes, sino también determinar exactamente el flujo de información, la disposición de las oficinas y sus componentes informáticos, las medidas de prevención en el tráfico de red, el almacenamiento de datos, su acceso, su proceso o posterior enrutamiento, medidas técnicas de contingencia y controles.
Al mismo tiempo, nos permitirá estar capacitados para recomendar los componentes necesarios de seguridad o conectividad como DMZ, firewalls, criptosistemas, routers, switchs, filtrados varios, IDS, databases, servidores seguros de archivos, servidores de logs, servidores de replicación, determinados enlaces cifrados, VPNs, VLANs, unidades de logueo seguro, cableado estructural blindado, etcétera.
Entre todo el material disponible, lo principal es conocer cómo se comunican estos elementos (sumado a los servidores y terminales) entre sí, sus capas, sus proto-

colos, su configuración y las normas técnicas de cada uno.



Visio. La aplicación Visio, del paquete Office de Microsoft, es muy utilizada para plasmar de forma gráfica la disposición de todos los componentes de un escenario informático. También sirve para diagramación lógica y organigramas, entre otros gráficos.

Conocer técnicas básicas de intrusión

> "Cuando estás empezando, no necesitas herramientas. Ése es el modo en que te volverás un script kiddie. Lo que necesitas es entender. Necesitas saber cómo trabajan los sistemas, qué errores pueden cometer sus programadores o administradores para que éstos se vuelvan vulnerables y cómo esos errores pueden ser explotados de modo que se pueda ingresar en el sistema.
> Una vez que entiendas qué es lo que estás haciendo, estarás preparado para elegir la herramienta correcta para la circunstancia correcta. Una vez que has elegido la herramienta, ésta sólo hará tu proceso más eficiente". **Derek Fountain (En: Bugtraq)**

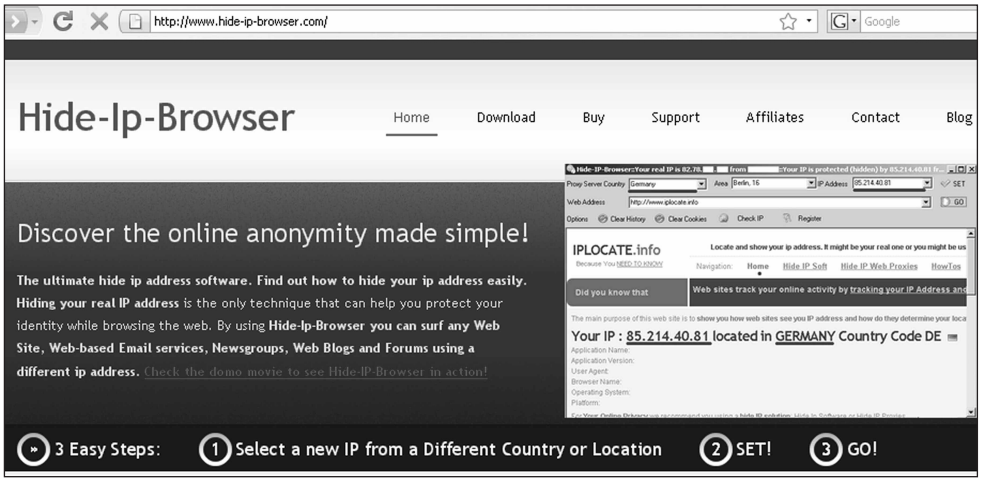
Antes de hablar de estas técnicas, debemos saber qué se entiende por **intrusión**. Para definirlo de un modo simple, significa lograr el acceso a recursos de un sistema sin tener la autorización de su dueño o de quien lo controla. Quien lleve a cabo este tipo de accesos no permitidos es lisa y llanamente un **intruso**, sea como

fuere que lo cataloguen los medios, las autoridades o el resto de la gente.
Aunque existen muchas formas de intrusión, aquí veremos ejemplos del ámbito informático, es decir, el ingreso de terceros no autorizados en la información (almacenada o en flujo) en **estado digital** de una organización. De todas maneras, debemos tener en cuenta que en el sistema de cualquier organización, los datos vitales suelen estar en una amplia gama de soportes, como papel, memorias diversas, cintas, audio, pizarras, paneles, ondas de radio, video, diapositivas y más. Varios de estos medios son llamados fungibles porque se agotan con su uso, como las cintas o el papel.
El intruso puede lograr acceso no autorizado a información de modo:

- Físico: **in situ**, estando frente a la máquina.
- Remoto, local o ambos a la vez.
- Por cable: vía Internet o línea telefónica.
- Por ondas: **wireless**.
- Por radiación: **eavesdropping**.
- Por vista u oído: a **distancia**.
- A través de una **interfaz gráfica**.
- A través de un **intérprete de comandos**.
- A través de un intérprete de comandos a ciegas, sin ver el resultado de lo que se ejecutó en el servidor remoto.

Entrar no solo significa introducir el usuario y la clave en un determinado servicio de autentificación remota como telnet, ssh, terminal service, rlogin, ftp, y todos aquellos que soliciten ingresar validación. Puede significar la realización de una **escalada**, que consiste en una sucesión de actos que llevan a lograr cada vez mayor alcance dentro del sistema para, finalmente, obtener una cuenta de elevados privilegios o el propósito que se haya impuesto el ejecutor. Por ejemplo, enviar por email o ftp determinado archivo o database al exterior, agregar un usuario de privilegios en el sistema o, simplemente, entrar y ocultar su rastro para que en el futuro se pueda utilizar ese servidor para otros propósitos. Esto podría llevar meses o minutos, y las más variadas técnicas, ya sea a través del mismo sistema operativo, de alguna aplicación o de algún descuido del administrador (hablamos siempre de servidores con administrador y no de simples terminales de usuarios con Windows XP).
Sin dudas, un intruso se aprovechará de los descuidos humanos, ya que todos los componentes del sistema fueron desarrollados, seteados u organizados por personas; por eso tienen falencias que son potencialmente explotables. Entonces, ¿cuál es la mejor forma de aprender técnicas de intrusión? En principio, conocer el objetivo, empezando por el sistema operativo (con esto no hacemos referencia a elementos del tipo Windows 98, sino a Linux, la familia BSD y la familia Windows Server).

Los descuidos de administración son difíciles de descubrir y explotar si no se conoce profundamente el sistema operativo o la aplicación en sí. Imaginemos el tiempo que llevaría aprender, sobre la marcha de un chequeo, las características de un sistema operativo (y sus aplicaciones) o todos los componentes de un escenario.
Hay que estar informado acerca de las nuevas **vulnerabilidades** o descubrirlas por uno mismo si se tiene el tiempo para hacerlo, siendo muy útil la habilidad de encontrarlas y poder programar su **exploit** (prueba de concepto). También es bueno saber cómo identificar un sistema y reconocer si es potencialmente explotable su modelo, versión o estado. Para ello, podemos recurrir a los incontables libros y whitepapers, honeypots, wargames, concursos, listas de correo profesionales, e-zines y foros serios. Además podemos montar una red hogareña para practicar, máquinas virtuales en ***Vmware*** o hacerlo en el trabajo si es posible.



IP. Hide-Ip-Browser (www.hide-ip-browser.com) es un software que permite mantener el anonimato al navegar sitios y al postear en foros. Esto lo realiza mediante la elección de diferentes servidores proxys.

Sobre los cursos que se ofrecen en Internet, ya sean de seguridad o de ethical hacking, hay que tener en cuenta que por estos días, la Web es masiva y hay muchos

Listas de Correo

En estas listas de correo nos ayudarán a encontrar respuestas a nuestras preguntas: www.segu-info.com.ar, en español (forosi); www.issaarba.org, en español (ISSAArBA); www.securityfocus.com, en inglés (Bugtraq/Security Basics); www.infosecnews. org, en inglés (ISN); www.elistas.net/lista/nnl, en español (NNL Newsletter).

empresarios que brindan dudosos cursos (obsoletos o incompletos) para así aprovecharse de la ignorancia de la gente y ganar dinero. Esto no significa que todos los cursos son malos, pero en gran parte son una pérdida de recursos. Para no correr riesgos, es bueno tomar estos recaudos:

1. Dentro de una lista de correo de seguridad, preguntar a los profesionales cuál sería el curso adecuado según nuestro nivel, interés, fin o recursos económicos.
2. Evaluar, tras haber hablado con alguien que haya cursado allí, cuáles fueron los costos totales, las horas, el alcance, si tienen programa o entregan material de estudio, cuál es el seguimiento del aprendizaje, qué clase de título o certificado entregan al finalizar y qué reconocimiento tiene éste en el mercado laboral local o mundial. También sería bueno saber si la persona que nos informa quedó conforme y en qué aspectos el curso fue flojo, o no se cumplió con lo prometido.
3. Comprobar la experiencia real en seguridad de quien o quienes imparten el curso o el programa de estudio que está por pagarse. No está mal pedir referencias o currículum vitae, y en lo posible conviene hacerlo de modo formal, por teléfono o en la oficina misma.

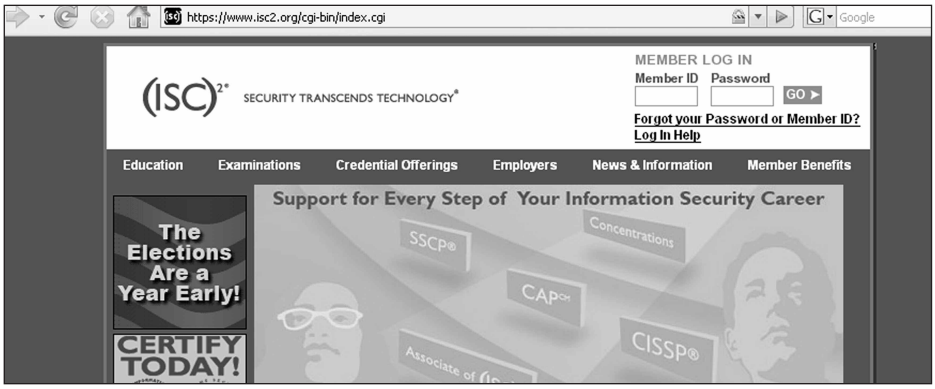
Educación formal

Hoy en día, no existe una carrera de grado formal de nivel universitario (de varios años de duración) sobre seguridad informática que comprenda, en su contenido, al ethical hacking de modo práctico (**hands on**). Apenas hay algunos postgrados, certificaciones y tecnicaturas relacionadas. Sí hay carreras como analista de sistemas, ingeniería en sistemas, licenciatura en sistemas, doctorados, especializaciones y maestrías, que son buenos formadores **de base** para la materia. Allí se estudian las tecnologías comprendidas en los sistemas, protocolos, sus procedimientos, técnicas, diseño y organización. El estudio formal, de alguna manera, modelará todo lo que aprendamos de manera autodidacta, y no sólo en relación con los contenidos de las materias, sino también porque enfrentarnos a numerosos exámenes escritos y orales nos dará cierto temple ante pequeños desafíos reales, de resolución analítica.

Lecturas adicionales

Es recomendable leer libros de Auerbach, la serie Hacking Exposed, de McGraw-Hill, de Sybex, de O'Reilly, de CRC Press, de Syngress, de Actualtests, de Learnkey, todos los de temática CISSP, los 31 ejemplares de Hackxcrack y hackin9. Además, es interesante ver: www.zipsites.ru/books/edocs/edocs_list.php y www.insecuremag.com

Como si fuera poco, también se obtienen otros puntos de vista que servirán para abordar problemas, se conocen colegas que en algunos aspectos pueden ser más experimentados, se practica en laboratorios o entornos de red, se forman contactos de trabajo y estudio, se escuchan anécdotas y experiencias muy valiosas por parte de profesores o compañeros, entre otras cosas.
La educación formal es muy tenida en cuenta por las consultoras de RRHH gracias al **título** que brinda. Muchos autodidactas han sido rechazados por no poseer título alguno, sin siquiera tener la posibilidad de demostrar sus habilidades aun siendo excelentes **pentesters** y analistas.
En cuanto a las **certificaciones de seguridad**, hay más de 20, como podemos ver en **http://certification.about.com/od/securitycerts/a/seccertessentls.htm**. Algunas son consideradas como requisitos en determinadas organizaciones por su departamento de recursos humanos, pero como todo título, pueden no ser el verdadero reflejo de la capacidad y preparación de quien lo posee.



ISC. (ISC)2 es reconocida en todo el mundo por certificar profesionales CISSP. Fundada en 1989, pasaron por sus exámenes más de 50.000 profesionales. Su dirección es www.isc2.org.

En la preparación de estos exámenes, suelen aprenderse cosas interesantes o totalmente desconocidas, y es recomendable que todo aquel interesado en sumar experiencias

Ejercicios de programación

En http://community.corest.com/~gera/InsecureProgramming, podemos encontrar ejercicios de programación avanzada relacionada a fallas. Esto es útil ya que, cuanto más practiquemos (programemos), mejor serán nuestras habilidades para resolver problemas mediante programación.

en seguridad tome estos exámenes de certificación por una cuestión formal. Esto le permitirá ser un mejor candidato en las selecciones de los departamentos de recursos humanos.
A continuación, podemos leer parte de las declaraciones de **Iván Arce** (CTO de Core Security Technologies) acerca de la formación del profesional de seguridad, y más precisamente sobre las certificaciones de seguridad. La entrevista completa se puede leer en **www.acis.org.co/fileadmin/Revista_96/entrevista.pdf** (Gracias Iván por autorizar su reproducción).

- ¿Cómo se manejan las certificaciones, cuál es su alcance y aplicabilidad real en las empresas?

Difícilmente, una certificación de seguridad es un indicativo de la capacidad, experiencia o conocimiento real de un individuo en la materia. A lo sumo, es un indicativo de la existencia de algún tipo de formación básica en el tema, siguiendo la pauta del programa particular que puede ser malo, mediocre o medianamente bueno.
Un experto en seguridad informática no se forma como resultado de la acumulación de cursos y certificaciones, sino de la acumulación y la aplicación de una disciplina de trabajo y de estudio adquirida en otro contexto -escuela, universidad, trabajo, casa, etc.-, combinada con las capacidades creativas, de innovación, perseverancia y adaptación, propias de cada individuo.
No obstante, eso no impide que las certificaciones se adopten y se usen como un indicador de capacidad profesional y principalmente como un mecanismo del mercado laboral y de capacitación profesional, para establecer jerarquías, niveles salariales, planes de capacitación y justificar diversos tipos de decisiones y proyectos. -

Es muy importante que en el método formal de estudio no se estudie memorizando los contenidos sin llegar a comprenderlos, ya que en el momento de enfrentar la problemática, esto complicará realmente las cosas.
En el trabajo, esto es importante porque no se puede estar googleando en me-

Cómo saber qué carrera elegir

Consultando a profesionales en listas y dándoles detalles. Por Ej., si alguien desea dedicarse al cifrado de datos, es probable que le recomienden una licenciatura en matemáticas. A quien desea dedicarse a escribir procedimientos o normativas, le dirán que estudie Analista de sistemas de información, que posee materias como Organización y métodos.

dio de una intrusión de terceros en algún componente del sistema de la organización o en medio de una reunión ejecutiva. En un examen, porque los profesores se darán cuenta de que se está recitando un contenido de memoria, ya que tienen experiencia en escuchar alumnos o leer sus textos año tras año, y es un grave error subestimar a un profesor de esa manera.

Buscador. Universia (www.universia.com.ar) es el buscador más conocido de carreras online, a distancia o presenciales de nivel universitario o terciario en toda Latinoamérica.

CCNA

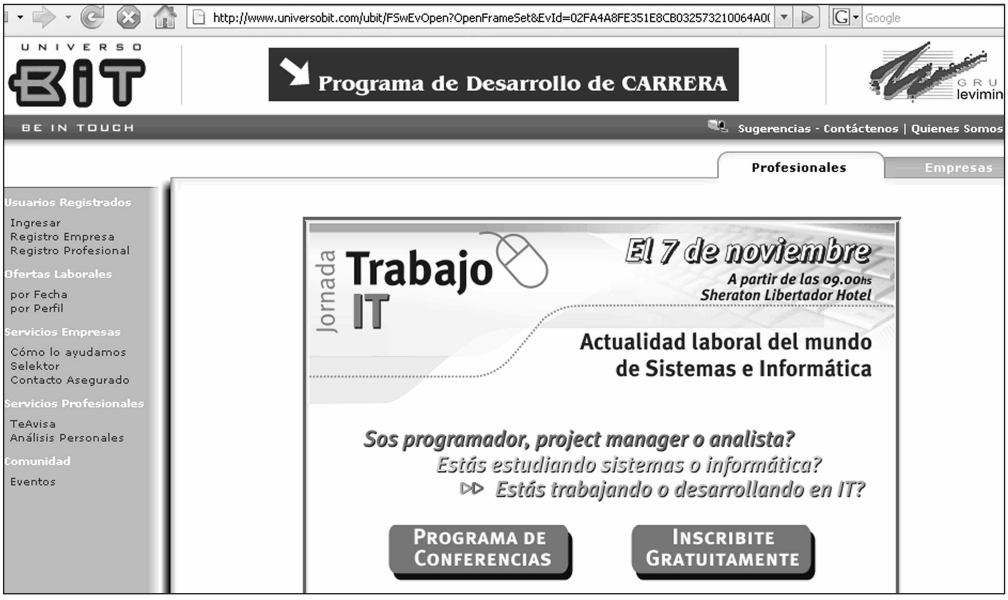
Significa Cisco Certified Network Associated y es una certificación de Cisco relacionada a networking. Los contenidos están relacionados con los modelos OSI y TCP-IP, cableado estructurado básico, enrutamiento, configuración de routers, switching, configuración de switches, VLAN, y tecnologías WAN. Más información en www.cisco.com

Trabajo & práctica

Nadie nace sabiendo, la práctica hace al maestro.

Anónimo

Mediante práctica y trabajo se va adquiriendo experiencia real y conocimiento sobre el tema. Se logran y mejoran las metodologías propias de trabajo, se conocen nuevas fuentes, tecnologías y maneras de abordar un desafío. No se puede comparar a alguien que conoce algo por haberlo enfrentado, con alguien a quien sólo se lo han explicado o que lo leyó. Esto es así porque de la teoría a la práctica hay algo que se llama **realidad**, y ésta suele transformar los resultados esperados.



Trabajo. El sitio www.jornadastrabajoit.com.ar se dedica a reunir jóvenes postulantes para algún trabajo o proyecto IT y ponerlos en contacto con reclutadores de las mejores firmas.

Lectura recomendada

Para obtener más conocimientos acerca de las organizaciones, es recomendable leer el excelente libro Técnicas de organización, sistemas y métodos, de Alberto R. Lardent (old school de la organización) y Claves para el desarrollo de la empresa, de Fernando Grosso, más ligado a las e-organizaciones de hoy en día y las nuevas prácticas.

Hay que tener en cuenta que no sólo por hacer un curso de hacker se es hacker, ni por rendir una certificación de seguridad o porque nos asignen un trabajo de chequeo de seguridad se es un profesional. El sacrificio de llegar a ser un profesional es realmente alto, y las consecuencias que padecen las organizaciones por no dar con uno acorde a la situación, no son tan buenas. De allí la gran importancia que tiene el reclutamiento de los profesionales por parte de la organización.

ORGANIZACIONES FORMALES

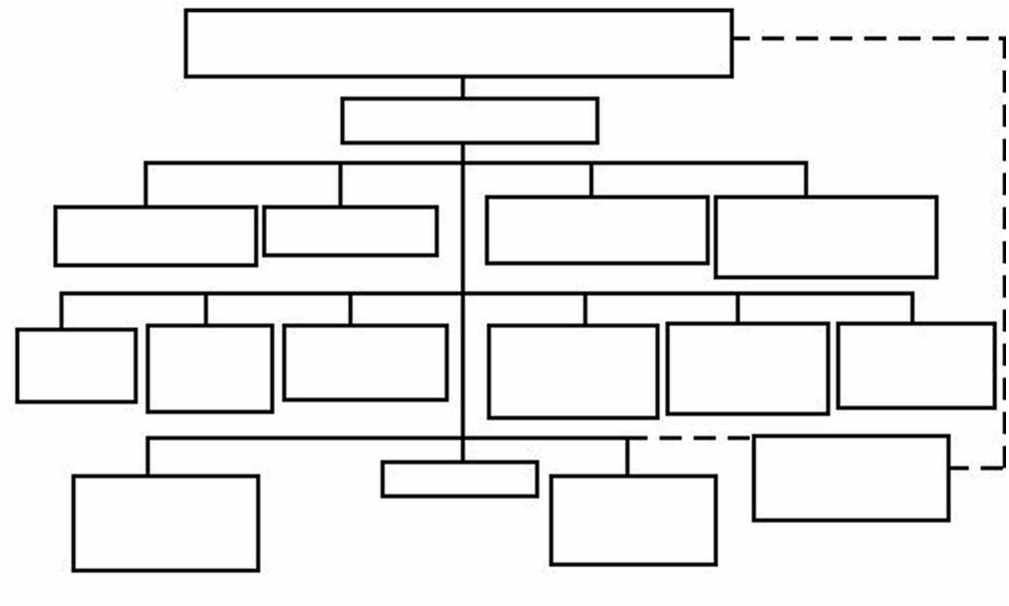
> *El hacking ético se ha convertido en una herramienta para formular un reconocimiento de las vulnerabilidades que representan una amenaza a los activos. El testeador está actuando como amenaza (hacker), en busca de las vulnerabilidades que permitirán la exposición de un activo, como ser: números de tarjeta de crédito. Al hacer eso, la prueba tiene el potencial de revelar los elementos fundamentales necesarios para crear una medida comprensiva y así emplear seguridad a través de una organización.*
>
> **James S. Tiller**

Las llamadas **organizaciones formales**, tal como nos enseñan en la teoría académica de cualquier carrera orientada a sistemas, son aquellas empresas que persiguen un objetivo a través de procesos administrativos, gestión de información y producción de elementos o servicios para colocar en un mercado sobre determinado contexto, siempre de modo legal y coordinado.
El común de la gente suele llamarlas grandes empresas, corporaciones o instituciones, y en este apartado enunciaremos algunos de sus aspectos principales para dar una noción muy básica de ellas, siempre que tengan una relación o interacción con el uso de ethical hacking, ya que éste es empleado en organizaciones formales. Estas organizaciones poseen, entre otras cosas:

Postularse para entrevistas de trabajo

En las siguientes direcciones: www.universobit.com, trabajoensistemas.com.ar, empleos.clarin.com, bumeran.com.ar, www.zonajobs.com.ar, www.computrabajo.com.ar, issaarba.blogspot.com (ver listado de consultoras) y www.tecnoempleo.com

- Diferentes áreas: operativas, administrativas/ejecutivas y gerenciales.
- Un flujo de datos e información vital y, por tanto, también un almacenamiento de éstos y un procesamiento.
- Recursos humanos, técnicos y lógicos.
- Responsables.
- Procesos.
- Estructuras jerárquicas sujetas a sectores y dependencias (mirándolo en un organigrama, desde arriba hacia abajo irán órdenes, y de abajo hacia arriba irá información de resultados).



Jerarquías. Organigrama de ejemplo. Estos definen la estructura organizativa y están tipificados bajo una norma IRAM. Puede hacerse por procesos, departamentos o sectores, jerarquías y productos.

Estas organizaciones, dentro de lo que es su **sistema** (llamado vulgarmente escenario) e integridad física total, poseen elementos vitales llamados **activos**, como lo es la **información sensible o crítica**. Los activos son muy variados y deben clasificarse tanto en tipo o número como en importancia (criticidad), aunque sólo haremos foco en el más importante. Para eso, primero debemos comprender que no es lo mismo hablar de datos que de información, ya que ésta última tiene una importancia significativa para la empresa. Por ejemplo, como información sensible o crítica podemos mencionar:

- El listado de clientes con todos sus datos.

- Listado de proveedores, compradores, socios.
- Claves o contraseñas.
- Ubicación de puntos de acceso privados.
- Planos.
- Información crítica o confidencial de tratados, negociados, reuniones, pautas, pactos.
- Combinaciones de cajas fuertes.
- Agendas, rutinas de horario, procesos.
- Inventarios, planillas de venta, compra y stocks.
- Listado de identidades de agentes.
- Información: personal, catálogos de productos futuros, costos, estadísticas, sondeos de mercado, balances privados, resultados, diseños, resultados de análisis, estrategias, participaciones, acciones, materiales, fórmulas de productos, ecuaciones, grabaciones digitales, tesis, fotos y films privados, investigaciones, nóminas de pago, entre otras tantas cosas importantes.

Podemos imaginar muchas situaciones que pueden atentar contra estos activos de la empresa. Por ejemplo, que un intruso o malware tenga acceso a ellos, que los alteren o los borren para siempre o que los entreguen a la competencia o al mejor postor. También existe una enorme cantidad de amenazas naturales, técnicas y humanas (como un empleado desleal que la roba o copia, por ejemplo) que podrían atentar contra ellos. Lógicamente, en estos tiempos de alta competitividad, el impacto negativo sería muy grande. De todas maneras, debemos recordar que la información crítica es tan solo uno de los activos que hay que proteger, de los tantos presentes en una organización.

Actualmente, las organizaciones necesitan seguridad a través de la incrementación de la calidad en sus procesos y el resguardo de sus componentes (activos), a través de estándares, normas, políticas, controles, seguimiento y la mejora continua de éstos. Para ello se practican **auditorias** de seguridad IT, **relevamientos** exhaustivos, y **revisiones** de los procesos, funciones y tareas relacionadas con las buenas prácticas en seguridad. Todo ello hace a la **gestión de la seguridad de la información**, como veremos en el capítulo 9, que explica en un punto el tema normativas.

No hay que confundir la gestión de la seguridad de la información con la **segu-**

Material acerca de políticas

Si queremos obtener más información sobre políticas y estudiar profundamente sobre ellas, podemos visitar los siguientes sitios:
www.segu-info.com.ar/politicas (hay que registrarse en la lista Segu-info) y
www.segu-info.com.ar/articulos/59-escribiendo-politicas-seguridad.htm

ridad informática en el aspecto técnico. Una cosa es reforzar técnicamente la seguridad de un servidor mediante **hardening,** y otra es, por ejemplo, redactar una política de uso de Internet de modo seguro y responsable por parte de los empleados. A continuación, veremos algunos de los descuidos típicos con los que una organización formal cuenta:

- La OF ha crecido de modo desordenado y, por si fuera poco, está en extremo informatizada, sin seguridad mínima o normativa de organización alguna. Es el típico caso de incontables empresas familiares que, por diversos factores político-económicos, crecen hasta ser grandes exportadores o importadores, o bien industriales manufactureros, y agrandan su sistema informático al ritmo de su personal sin lógica alguna, sustentando la seguridad con sólo actualizar el sistema operativo de sus terminales y utilizando algún que otro antivirus, desactualizado. Muchas de estas empresas saben que tienen que implementar seguridad informática y de la información, pero no saben cómo abordarlo.
- La OF está acostumbrada a la reacción y no a la proacción (actuar de modo anticipado). Aguarda a que suceda algún incidente para hacer algo, antes de implementar algo de modo seguro y sin haber comprometido nada por omisión, desinterés o descuido. Muchas de estas empresas simplemente no se interesan en la inversión previa en cuestiones de seguridad, a menos que se hayan dado cuenta de algún incidente de ese tipo, cuando ya es demasiado tarde. No son conscientes de los beneficios que tiene para la organización el **penetration testing** o chequeo de seguridad (descubrir las vulnerabilidades del sistema antes de que éstas sean encontradas y explotadas por un tercero no autorizado u otra amenaza).
- La OF contrata personal de seguridad con un perfil inadecuado a su escenario y contexto. (más detalles sobre este punto en el Cap9)
- La dependencia de su departamento de seguridad hace ineficaces sus políticas. No logran la interrelación de sus sectores y no alcanzan el compromiso de la gerencia para que la totalidad del plantel acate las políticas, dando lugar a diferentes tipos de problemas. Uno de los interrogantes más comunes en estos casos es de quién debe depender el departamento Seguridad de la información.
- La OF no sabe abordar la redacción de las políticas de seguridad (o del análisis de riesgo) o su implementación. A veces se solapan con políticas de organización, con incidencia en la dinámica de la información intersectorial y comunicaciones.

Debemos recordar que la información significativa y a tiempo es vital para la toma de decisiones en lo gerencial, y a la vez decisiva para lograr los objetivos de la organización. El ethical hacking aporta el mecanismo para lograr canales (y repositorios) más seguros para esa información y otros activos.

NETWORK SECURITY ASSESSMENT

Adéntrate en la nada, acomete contra el vacío, rodea lo que defiende, asáltalo donde no te espere. **Sun Tzu**

(The Art of war)

En las páginas anteriores definimos los puntos más interesantes:

- El intruso como amenaza.
- La organización formal (OF) como sistema o escenario en riesgo.
- La gestión y el método organizativo como optimizadores de la OF.
- El activo como valor preciado de la OF.
- El hacking ético como herramienta o mecanismo.
- El profesional de seguridad como ejecutor del testeo.
- Las técnicas como parte del network security assessment.

El mayor contenido del libro se basa en este último punto, pero no podíamos llegar a él y ver sólo técnicas detalladas de testeo sin antes conocer de qué se trata el resto, ya que importante saber dónde encaja cada uno de estos componentes.

La red está llena de **script kiddies** (algunos de ellos si dejan de perder tiempo y estudian, podrían ser el día de mañana profesionales), y como no saben por dónde empezar, lo primero que utilizan es lo que tienen a mano: una herramienta o la descripción detallada de una simple técnica de intrusión que leyeron en algún correo o foro. Aclaremos que un script kiddie es aquella persona que, sin conocimiento alguno de protocolos, sistemas operativos, ni seguridad de la información, se vale de una herramienta o técnica ajenas para cometer intrusiones en Internet u otras redes, o al menos intentarlo. Lógicamente, puede tener las más diversas intenciones. Por otro lado, ***network security assessment***, es uno de los nombres que suele tener el penetration testing o chequeo de penetración, también conocido como **testeo de vulnerabilidades**, prueba de penetración o hacking ético, como suele llamárselo por estos días. El beneficio de éste para la organización es que ella se conozca a sí misma en cuestiones de vulnerabilidades y potenciales brechas de seguridad en el sistema de información, emulando en ataques tanto a script kiddies como tambien, a hábiles intrusos.
Este chequeo de seguridad puede ser **externo** si es desde Internet hacia un sitio web de e-commerce o hacia terminales de una red corporativa o componentes de ésta; o **interno** si es desde de una misma red, emulando un empleado o bien un intruso que ha logrado ingresar desde el exterior a la red interna de la organización. Es siempre de carácter técnico, al contrario de una auditoria de seguridad IT en la que se comprueban

o pasan a revisión las políticas y los procedimientos. También puede denominárselo como:

- **White Box Test**: es un chequeo llevado a cabo por un pentester que tiene toda la información acerca del sistema.
- **Black Box Test**: este chequeo es llevado a cabo desde cero, sin información, tal como lo haría un intruso cualquiera y lleva mucho más tiempo.
- **Grey Box Test**: se cuenta con conocimientos parciales del objetivo, siempre brindados por la misma organización.

Generalmente, las organizaciones se alinean bajo alguna metodología para realizar el testeo, aunque otras más versátiles optan por hacerlo de modo más artesanal, lo cual no significa gran diferencia siempre y cuando el profesional sepa dirigir el assessment (ataque) adecuadamente y no deje objetivos, detalles o tramos olvidados.

Materia. En el programa de 5º año de Ingeniería en Sistemas, la Universidad Abierta Interamericana (www.vaneduc.edu.ar/uai/) posee la materia Seguridad Informática. Comprende: cifrados, seguridad de la información (análisis de riesgo, contingencia, auditorias), detección de intrusos, seguridad en red, filtrado de paquetes y firewalls, hacking y administración segura de plataformas y aplicaciones (hardening).

Para evitar circunstancias indeseadas, existe la planificación previa, que sirve para determinar el alcance que tendrá, los límites, los objetivos y la buena utilización de recursos. En muchos casos, se discute quién debería llevarlo a cabo, si personal propio de la organización o terceros contratados. Para tomar esta decisión, entra en juego la **ética** de los integrantes del departamento de sistemas y el de seguridad informática, dado que tienen que reportar fallas o implementaciones deficientes, quizá llevadas a cabo por colegas de la misma oficina. Hay que prestar suma atención a los conflictos de intereses que pueden crearse en empleados, administradores y analistas de una misma empresa en una búsqueda de estas características.

Al ser analista **externo**, generar un reporte de seguridad detallado es una incógnita para los empleados de seguridad o sistemas de la organización que nos ha contratado, hasta que se entrega. La ética difícilmente pueda ser menoscabada, aunque los recursos utilizados (tiempo, herramientas, dinero y recursos humanos) suelen ser mayores.

Al ser analista interno, se facilita la tarea porque se conoce mejor y de modo real el sistema de información, y por tanto disminuyen los recursos utilizados y se complica en otros aspectos. En algunas organizaciones es muy común que, al encontrar algo, se avise al colega administrador o analista para que lo solucione y así no figure en el reporte. Si bien eso sería mitigar rápido el problema, es una falta de ética profesional y un ejemplo de innumerables vicios relacionados.

Lo más recomendable es que se implemente todo de manera correcta y, en lo posible, que se desarrolle el sistema desde cero. Luego de realizar relevamientos exhaustivos, conviene que se planifique y se definan los procesos adecuadamente (hasta la dependencia más primitiva), ya que en el transcurrir del tiempo deberán ser siempre depurados. También hay que tener en cuenta la escalabilidad a futuro y un plan de contingencia para asegurar la continuidad del negocio y el procesamiento de datos.

La idea es llegar a un nivel de organización y de seguridad maduro que sea auditado y chequeado por analistas externos junto a analistas de organización y métodos. Crear un comité para debatir los resultados e implementaciones, y mitigar las falencias encontradas de modo serio. Controlar y auditar para mejorar, reclutar verdaderos talentos y formarlos más aun en la empresa.

Todo esto es valor agregado en la búsqueda del objetivo por parte de la organización, por tal motivo, hay que tratar de cumplir muy bien nuestro rol si vamos a dedicarnos de lleno al tema.

Sitios de Educación.

www.sistemas.frba.utn.edu.ar
www.caece.edu.ar/Grado/Ing_Sistemas.asp
www.isec-global.com
www.rsa.com/training/pdfs/EDCRS_GD_1004.pdf
www.checkpoint.com/services/education/certification
www.cisco.com/web/learning
www.comptia.org
www.itmaster.com.ar
www.itcollege.com.ar

www.centraltech.com.ar
www.cybsec.com/ES/servicios/capacitacion.php
www.bs.com.ar
www.proydesa.org

Noticias

www.derkeiler.com
www.net-security.org
www.seclists.org
www.securitytracker.com/signup/signup_now.html
www.microsoft.com/technet/security/
www.kernel.org/pub/linux/docs/lkml/
http://lists.grok.org.uk/pipermail/full-disclosure
www.hispasec.com
www.securiteam.com/mailinglist.html
www.whitehatsec.com

www.segu-info.com.ar

Es un sitio dedicado a la seguridad de la información con una gran comunidad. Cuenta con varios mailing lists, y los temas centrales de éstos son la seguridad de la información, la seguridad informática y las leyes relacionadas con la seguridad de la información. Se llevan a cabo tanto discusiones entre profesionales como concientización sobre seguridad a gente que utiliza recursos tecnológicos e Internet.