USERS

Técnico en

REDES &SEGURIDAD

1

ETHICAL HACKING

CONOZCA LAS TÉCNICAS DE ATAQUE DE LOS PROFESIONALES DE LA SEGURIDAD

- PRUEBAS DE PENETRACIÓN
- SEGURIDAD FÍSICA
- INGENIERÍA SOCIAL
- CRIPTOGRAFÍA Y PASSWORD CRACKING

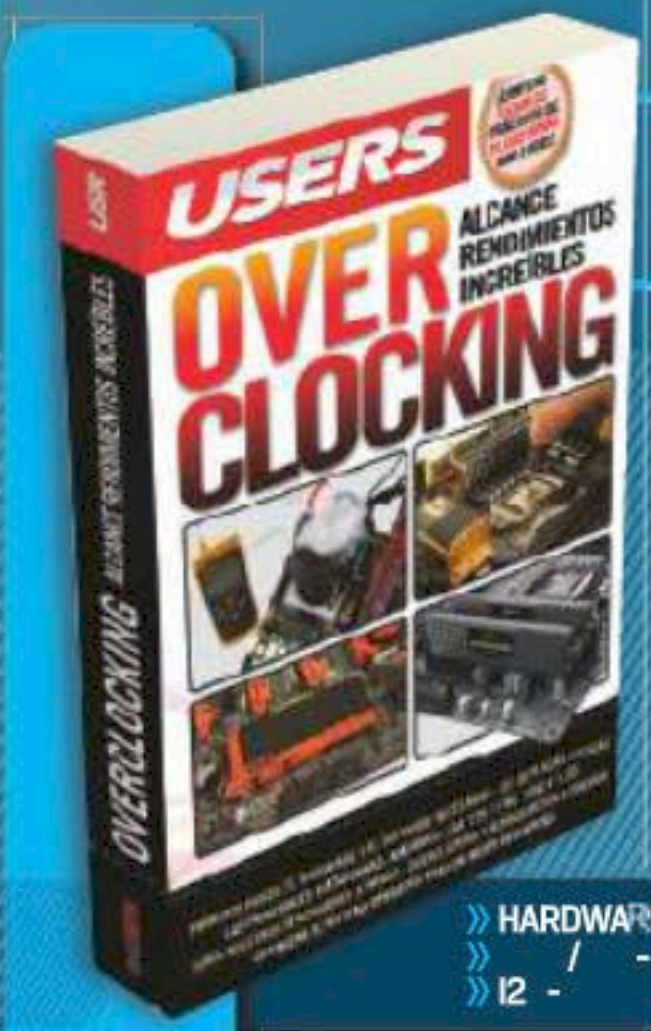
CONÉCTESE
CON LOS MEJORES LIBROS DE COMPUTACIÓN

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

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

CAPACÍTESE PARA OBTENER UNA MEJOR SALIDA LABORAL

» HARDWARE / MOBILE
» / - 2
» 12 -



ALCANCE RENDIMIENTOS INCREÍBLES EN SU PC

» HARDWARE
» / - 2
» 12 -

APRENDA A PROGRAMAR SIN CONOCIMIENTOS PREVIOS

» DE2 ARROL .
» / I- 2
» 2 -

ACCEDA A SUS DOCUMENTOS EN TODO MOMENTO Y LUGAR.

» /1 2 2 -31- 3
» / I- 2
» 2 -

USERS

Técnico en REDES &SEGURIDAD

TÍTULO: Electrónica elemental
COLECCIÓN: Pocket Users
FORMATO: 13.5 x 19 cm
PÁGINAS: 96

Primera impresión realizada en junio de MMXII.

Sevagraf, Costa Rica 5226, Grand Bourg, Malvinas Argentinas, Pcia. De Buenos Aires.

ISBN 978-987-1857-50-0

Coordinado por Paula Budris
Electrónica elemental - 1a ed. - Buenos Aires : Fox Andina; Dalaga, 2012.
96 p. ; 19x13 cm. - (Pocket users; 22)
ISBN 978-987-1857-50-0

1. Informática. I. Budris, Paula, coord.
CDD 005.3

VISITE NUESTRA WEB

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

RedUSERS
COMUNIDAD DE TECNOLOGIA

redusers.com

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

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

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

usershop.redusers.com usershop@redusers.com + 54 (011) 4110-8700

Prólogo **al contenido**

Cuando pensamos en seguridad informática probablemente se nos vengan a la cabeza una serie de ideas entre las que se encuentran los hackers, los ataques por Internet, la privacidad, las contraseñas y otras tantas cosas. La información que hay dando vueltas puede ser confusa en ciertas ocasiones. De este modo, suelen surgir algunos interrogantes en quienes desean adentrarse en este mundo: ¿es algo que se estudia? ¿Existen los hackers realmente? ¿Cómo se puede trabajar en seguridad informática? ¿Qué hace un profesional de la seguridad? ¿Puede el hacking ser ético? Con esta batería de preguntas y algunas más, cualquier entusiasta comienza la carrera hacia el conocimiento de la temática, una carrera que no cesa de traer nuevos desafíos con el tiempo.

Lo cierto es que la seguridad informática propone un modo distinto de ver la realidad, casi una filosofía de vida. Es una disciplina en la que resulta imposible adentrarse sin recurrir al sentido de la curiosidad y la creatividad.

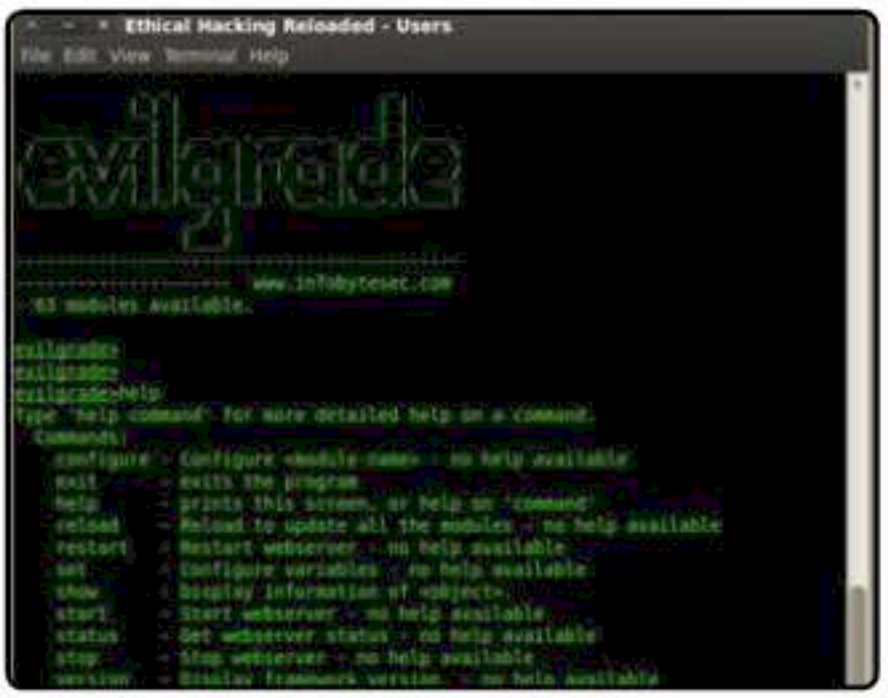
A través de cada uno de los capítulos de esta obra hemos intentado cubrir los temas fundamentales que hacen a la seguridad informática orientada al ethical hacking como proceso de evaluación de la seguridad, comenzando por la más elemental introducción a los conceptos necesarios, pasando por la explicación de las distintas fases de un ataque, subdividida en etapas más simples, y por las técnicas de ataque fundamentales en redes e Internet, hasta llegar a temas más específicos, como la criptografía. También abordamos aspectos menos técnicos pero no menos importantes, en capítulos dedicados a los ataques sin tecnología, como la ingeniería social y la seguridad física.

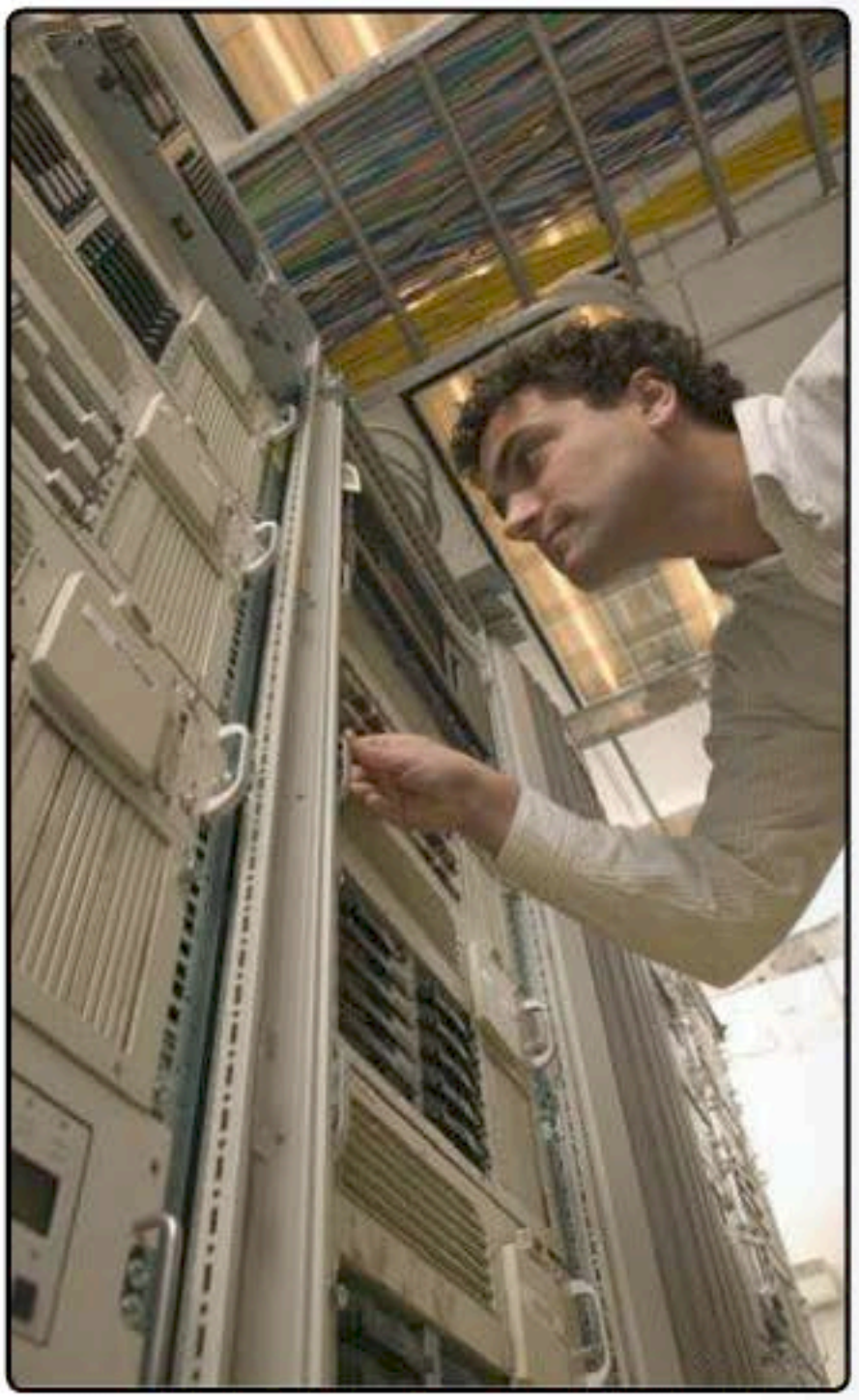
Los temas son tan amplios y variados que es imposible no dejar algunos afuera, por lo que hemos tenido que realizar una cuidadosa selección de manera tal que nada importante quede sin tratar.

Esperamos que disfruten esta obra y que pueda ser fuente de referencia y punto de partida para introducirse en este tema tan misterioso. Sean bienvenidos al universo del ethical hacking.

Federico Pacheco
info@federicopacheco.com.ar

Contenido **del libro**





Capítulo 1

Introducción al ethical hacking

En este capítulo definiremos algunos conceptos que servirán como base para comprender el resto del libro.

RedUSERS.com

Ethical **hackers**

Cuando oímos estas dos palabras, lo primero que se nos viene a la mente son preguntas como: ¿quiénes son estos nuevos personajes, protagonistas de la escena mundial? Y por sobre todo: ¿qué conocimientos tienen?

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 él sabe, por lo que hace, 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 profundos conocimientos sobre los sistemas operativos, sabrá sobre hardware, electrónica, redes, telecomunicaciones, y también sobre programación en lenguajes de alto y bajo nivel. Además, entenderá sobre problemas relacionados con la seguridad en temáticas como la criptografía, los sistemas de control de acceso, las aplicaciones, la seguridad física y la seguridad administrativa.

Figura 1. Antitrust **es una conocida película sobre tecnología en la que el hacking ético se utiliza para adueñarse de la gloria.**

Un ethical hacker seguirá un estricto código de conducta, dado que de eso se trata la primera parte del concepto. 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 esto 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, de una gran dosis de humildad.

Por si no ha quedado del todo claro hasta aquí, podemos definir por descarte lo que es

QUÉ NO ES UN ETHICAL HACKER

No es a quien una empresa contratará para robar la información de su competencia. No es quien investigará el e-mail de la pareja de alguien. No es quien se hará famoso por crear un virus. No es quien romperá un sistema para beneficio personal.

un ethical hacker. Esto evitará dar con perfiles equivocados, ya que muchas personas se autodenominan de esta manera o de alguna similar, sin llegar a serlo realmente. Está claro, que muchos querrían desempeñar su papel.

Sería agradable constatar que, llegado este punto de la lectura, aún no hemos echado por tierra las esperanzas de nadie de convertirse en un ethical hacker. Muy por el contrario, el único objetivo de esta disquisición es quitar el manto de irrealidad que muchas veces cubre los temas relacionados con el hacking y la seguridad de la información.

Códigos de ética

El prestigioso filósofo británico Bertrand Russell afirmó en su obra **Sociedad Humana: Ética y Política**: "En cada comunidad, incluso en la tripulación de un barco pirata, hay acciones obligadas y acciones prohibidas, acciones loables y acciones reprobables". A partir de esta afirmación, podemos decir que un pirata debe tener que mostrar valor en el combate y justicia en el reparto del botín; si no lo hace así, entonces no es un buen pirata.

Cuando un hombre pertenece a una comunidad más grande, el alcance de sus obligaciones y prohibiciones se amplía todavía más; siempre hay un código al cual se ha de ajustar bajo pena de deshonra pública.

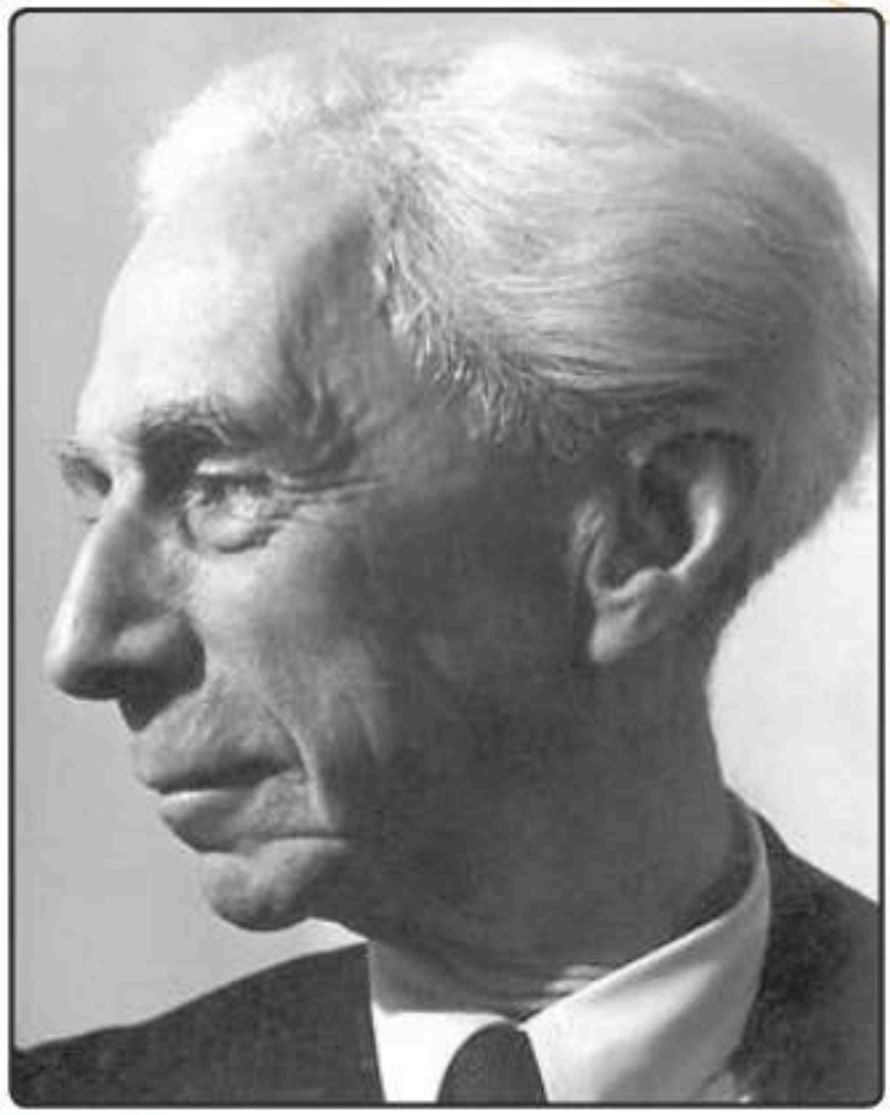


Figura 2. Bertrand Russell, **gran filósofo y matemático británico**

Este párrafo ilustra la necesidad filosófica de un código de comportamiento o de ética, que se crea con el objeto de ofrecer mayores garantías de solvencia moral y establecer normas de actuación profesional. Cuando una persona adhiere al código de ética de cierta organización o profesión, se está comprometiendo a obrar de modo tal de cumplir con los parámetros que han sido definidos por ella.

Más generalmente, y ya desde hace tiempo, se gestó una **ética hacker** propia, que se aplicó mucho a las comunidades virtuales. Un estudioso del tema ha sido el filósofo finlandés Pekka Himanen, que en su obra **La ética del hacker y el espíritu de la era de la información** (con prólogo de Linus Torvalds y epílogo de Manuel

Castells) rescata el sentido original del término y le otorga la valoración que hemos analizado anteriormente. Según Himanen, la ética hacker es una nueva moral que desafía **La ética protestante y el espíritu del capitalismo** (obra de Max Weber), fundada en la laboriosidad diligente, la aceptación de la rutina, el valor del dinero y la preocupación por la cuenta de resultados. Ante la moral presentada por Weber, la ética del trabajo para el hacker se funda en el valor de la creatividad y consiste en combinar pasión con libertad. El dinero deja de ser un valor en sí mismo, y el beneficio se asienta en metas como el valor social, la libertad de la información y la transparencia.

Clasificación de los hackers

Si bien hemos ya definido la palabra hacker, existen clasificaciones que distinguen el comportamiento de estas personas, haciendo referencia al color de su **sombrero** (hat) como característica de su perfil de personalidad.

Los **White Hat Hackers** son aquellas personas que poseen profundos conocimientos sobre hacking, que utilizan con fines defensivos. Aprovechan su saber para localizar vulnerabilidades en los sistemas e implementar contramedidas. Son llamados los **buenos muchachos** (good guys), y se encuentran del lado de la ley y la moral. También se asocia este concepto a los ethical hackers.

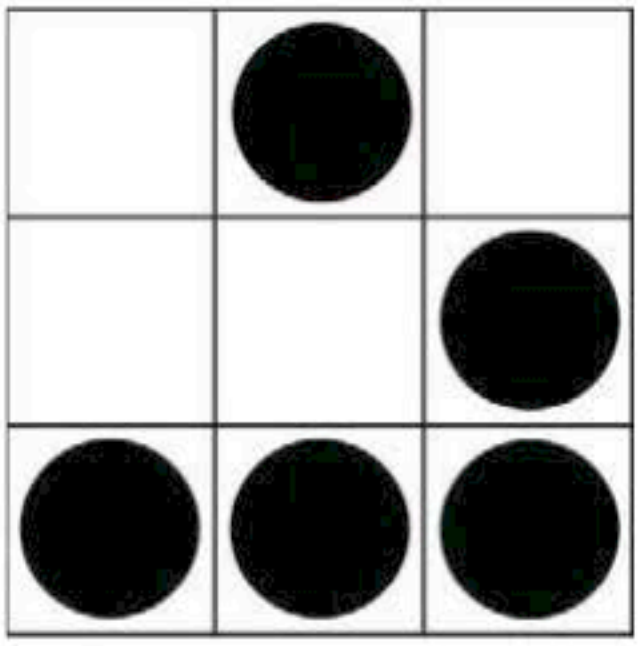


Figura 3. El emblema hacker, su uso expresa la solidaridad con los objetivos y también los valores de un hacker.

Los **Grey Hat Hackers por su parte** son personas que trabajan, por momentos, con una finalidad ofensiva y, en otros, defensiva, dependiendo de la circunstancia. Esta categoría plantea una línea divisoria entre hackers y crackers. Un Grey Hat Hacker ocasionalmente traspasa los límites. Una gran cantidad de personas transita durante mucho tiempo en esta vía, para luego encontrar asiento en alguno de los lados puros.

Figura 4. Brian May **fue reconocido por su "actitud hacker" por construir la guitarra que lo acompañó durante toda su carrera.**

Por último, tenemos a los **Black Hat Hackers quienes** están del lado opuesto a la ley y la moral. Son personas con un conocimiento extraordinario que realizan actividades maliciosas o destructivas. También son llamados los **chicos malos** (bad guys). Dentro de esta misma categoría podemos mencionar a los **Former Black Hats** (ex Black Hats), que poseen amplia experiencia de campo, pero escasa credibilidad, dado su oscuro pasado ilegal que no los apoya.

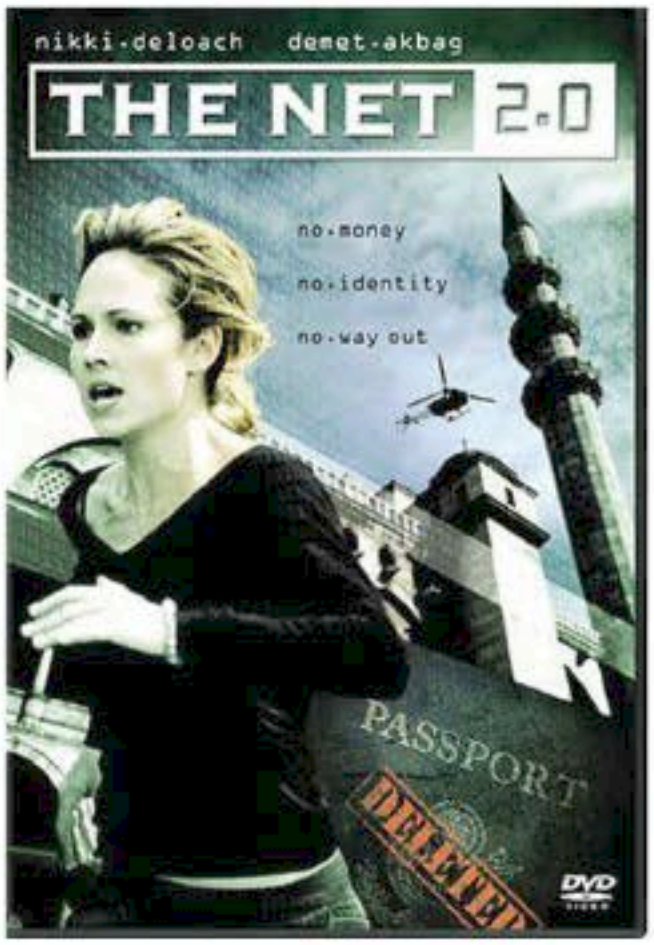


Figura 5. En La red 2.0 **, otro film tecnológico, se aborda la temática de los sistemas de seguridad y el robo de la información.**

Áreas 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.

Los primeros son los ataques al sistema operativo, que constituyen un punto 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 modo que, muchas veces, independientemente de lo que se encuentre por encima, se podrá explotar y tomar control del sistema en caso de que sea vulnerable.

En la actualidad, tenemos tres líneas principales: los sistemas del tipo **Windows**, los del tipo **Linux** o derivados de **UNIX**, y los sistemas **Mac OSX**, los cuales si bien están basados en UNIX, a esta altura presentan entidad propia. 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

¿ROMPER LA ÉTICA?

En general el rompimiento de alguno de los principios de un código de ética es penalizado con la expulsión de la persona de la entidad en cuestión, con la prohibición del ejercicio de la profesión y, cuando no, con el sometimiento a implicancias legales.

contar con su código fuente. Para el caso de Linux la situación es quizá peor, ya que, al poseer el código fuente, es posible detectar problemas también a nivel de código. Y en cuanto a OSX, la velocidad con la que ha acaparado mercado de múltiples plataformas en los últimos años, sumado a que los controles de seguridad implementados no son suficientes frente a las amenazas actuales, hacen que el sistema operativo de Mac sea un blanco cada vez más buscado por los atacantes. Pese a lo que se cree, la estadística de cantidad de vulnerabilidades de Windows no supera anualmente a la de Linux; en general, la diferencia ha sido la velocidad con la que aparecían las soluciones en cada caso, llevando aquí Linux la delantera. Respecto a Mac OSX, año a año la cantidad de vulnerabilidades que se descubren va en aumento.

Los ataques al sistema operativo también incluyen las implementaciones que este 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 tuviera un fallo en la implementación de cierta tecnología de cifrado, lo cual haría que el cifrado fuera débil, sin que se tratara de un problema en el propio algoritmo de cifrado ni en la aplicación que lo utiliza.

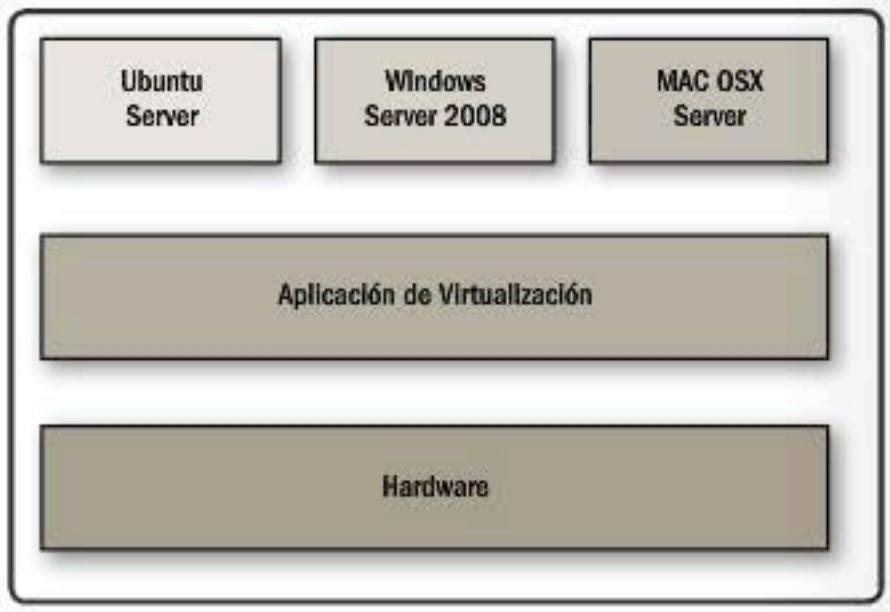


Figura 6. Cuando un sistema de virtualización es vulnerado, se pone en riesgo cada uno de los sistemas vinculados.

Estos ataques a su vez pueden ser locales o remotos y representan una pieza clave en la búsqueda de vulnerabilidades para el acceso a un sistema o a una red.

El segundo caso es el ataque a las aplicaciones, donde 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, necesariamente se producen errores. Para los ataques a las aplicaciones también se tendrá en cuenta la masividad de uso. Esto implica que un programa manejado por millones de personas para leer archivos del tipo **PDF** será

ENTORNOS VIRTUALES

Con la masificación de los entornos virtualizados, se agrega una capa para ser atacada. Es decir, además de los SO, también se puede atacar esta aplicación, con el problema de que su compromiso involucra el posible acceso a los sistemas virtualize.

mejor objetivo que uno empleado por unos pocos para editar cierto tipo de archivos específicos de un formato menos conocido.

Las aplicaciones amplían entonces la superficie de ataque de un sistema, por lo que se recomienda siempre evitar la instalación de aquellas que no se requieran, siguiendo el principio de seguridad que sugiere el minimalismo.

Figura 7. ICQ fue una aplicación pionera para la cual se desarrollaron programas que utilizaban su protocolo.

La idea de atacar la implementación de una aplicación en vez del software en sí mismo también vale para este caso. Muchos son los programas que realizan las mismas funciones, solo que algunos podrían hacerlo de manera tal que puedan encontrarse fallos en dicha operatoria, lo que comprometería al software, y con él, al sistema completo.

Justamente esta es otra de las problemáticas. Dependiendo de los privilegios con los cuales se ejecute 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, tema que analizaremos más adelante.

Figura 8. Sitio oficial del grupo Security & Privacy del IEEE (www.computer.org/portal/web/security).

En el caso de las configuraciones, ya sean del sistema operativo o de las aplicaciones, también encontramos 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: su configuración deficiente podría hacer que cumpliera su función de manera poco efectiva, provocando que una buena herramienta terminara por traducirse

en una mala solución y, por ende, en una brecha de seguridad.

Figura 9. En la pantalla podemos observar un conjunto de documentos del CSI (Center of Internet Security).

Si bien con el paso del tiempo la gran mayoría de los fabricantes han incorporado cada vez más medidas de seguridad en sus configuración de fábrica, un atacante, como primera medida, tratará de aprovecharse de las configuraciones estándar, ya sean aplicaciones, equipos informáticos, dispositivos de red, etcétera. Por ejemplo, si un panel de administración web se instala con un conjunto de credenciales de acceso por defecto y estas no son modificadas, cualquiera que conozca dichas credenciales podrá acceder. Esta es una clase de vulnerabilidad muy común, que puede ser aprovechada por cualquiera que posea mìnimos conocimientos tecnológicos.

Figura 10. Intypedia (www.intypedia.com) **es una enciclopedia de seguridad de la información desarrollada por la UPM.**

La solución más sencilla pero a la vez más efectiva para este tipo de problemas, sin dudas, es el **hardening**, que consiste en utilizar las propias características de los dispositivos, las plataformas y las aplicaciones implementadas para aumentar sus niveles de seguridad. Como, por ejemplo, cerrar aquellos puertos que no son imprescindibles para el establecimiento de las comunicaciones; deshabilitar protocolos y funciones que no se utilicen; fundamentalmente, cambiar los parámetros por defecto y también eliminar aquellos usuarios que no sean necesarios o que hayan quedado caducos son solo

LA FALSA SENSACIÓN DE SEGURIDAD

Ni siquiera las herramientas de protección y seguridad son fiables en sí mismas solo por su función. Esto podría producir algo muy grave que suele darse con frecuencia en el ambiente corporativo y el personal: una falsa sensación de seguridad.

algunas de las prácticas más habituales de un proceso de hardening. Como vemos, siempre podemos tomar precauciones para tratar de minimizar los riesgos de ataques.

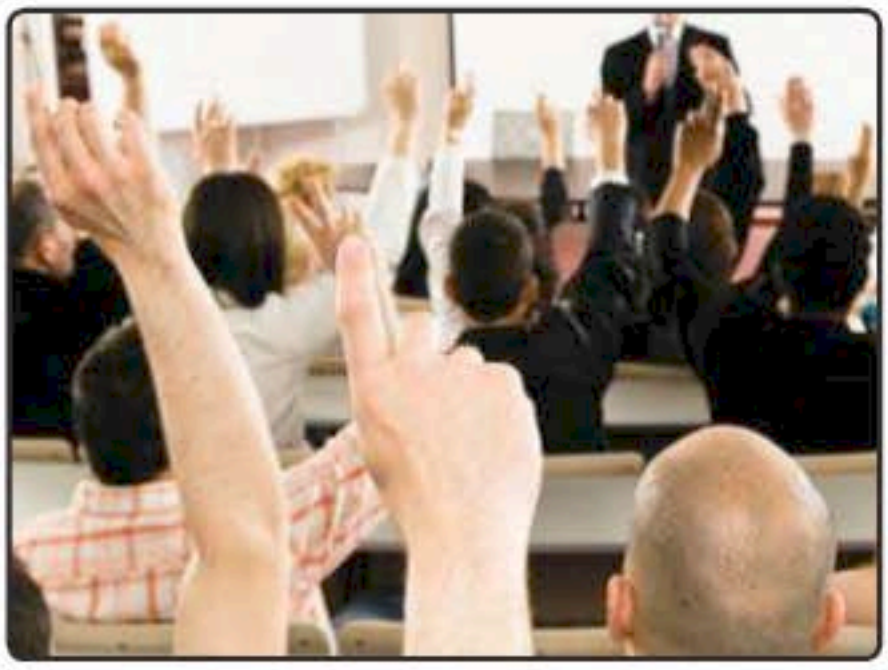


Figura 11. **Hoy día es posible tomar cursos para aprender ethical hacking, dictados por especialistas en el tema.**

Otro problema, tal vez más grave pero menos frecuente con el que podemos enfrentarnos, es que los errores estén directamente en los protocolos. Esto implica que, sin importar la implementación, el sistema operativo, ni la configuración, algo que se componga de dicho protocolo podría verse afectado. El ejemplo clásico es el **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 en uso. 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 uso, y con toda razón. Con el tiempo, su utilización 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 en un principio, de modo que se transformó en una verdadera arma de doble filo.

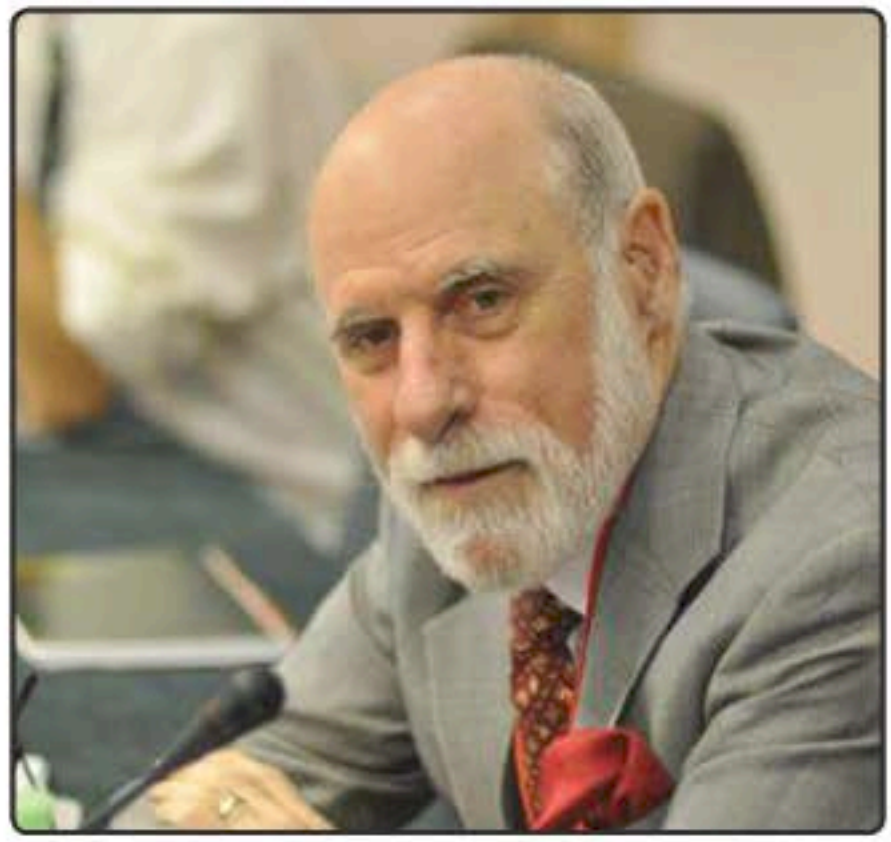


Figura 12. Vinton Cerf **fue el creador del protocolo TCP/IP, sobre el cual se basa la infraestructura de Internet.**

ESTÁ EN INTERNET

En Internet existen muchos sitios que presentan contraseñas por defecto de aplicaciones y dispositivos, como http://cirt.net/passwords. **En él encontraremos, clasificados por fabricante, una gran variedad de dispositivos con sus claves predefinidas.**

A pesar de esto, TCP/IP nunca ha estado en dudas, ya que todos las fallas se han ido corrigiendo o bien se mitigaron sus efectos a partir de las mejoras realizadas por las implementaciones; incluso, el modelo de referencia **Open System Interconnection (OSI)** se basó en él. Por otro lado, la masividad que tiene el protocolo hace que su reemplazo sea imposible en la práctica.

Figura 13. A fin de estar actualizados, es recomendable asistir a conferencias y charlas donde se trate el tema de ethical hacking.

Como podemos imaginar, dado que existen centenares de protocolos, hay, a la vez, muchas posibilidades de encontrar fallas en ellos. El problema más grave es que un error en el diseño de uno implica que las situaciones sean potencialmente incorregibles, y que deben realizarse modificaciones a distintos niveles para resolverlo, incluyendo 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 de protección para la que son utilizados.

RESUMEN

En este capítulo abordamos los conceptos fundamentales sobre ethical hacking, definimos el perfil del profesional que realiza estas tareas, clasificamos a sus colegas y propusimos una aproximación a las áreas sobre las que se enfocan los ataques.

Capítulo 2

La evaluación de la seguridad

En este capítulo analizaremos algunas de las evaluaciones de seguridad más implementadas en este momento.

RedUSERS.com

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.

En este sentido, no solo se remite a las tecnologías informáticas o 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, entre otros. De esta manera, se busca determinar las amenazas, los agentes de amenaza y las vulnerabilidades a los que está expuesto el sistema en su conjunto. Estas debilidades suelen referirse a todas aquellas 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 sobre 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, dispositivos, sistemas operativos, aplicaciones y un largo etcétera vinculado a todas las deficiencias técnicas posibles. Es importante destacar que este tipo de evaluaciones solo identifica potenciales vulnerabilidades, pero no confirma que estas existan. Dicho de otra forma, cuando se detecta una vulnerabilidad en un equipo o sistema, no se trata de explotarla para confirmar su existencia, sino que, simplemente, se la reporta.

Figura 1. El requerimiento 11 del PCI-DSS recomienda ejecutar una evaluación de vulnerabilidades cada tres meses.

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

EVALUACIONES ANUALES

Por lo general, las diferentes normativas de la industria exigen efectuar determinada cantidad de evaluaciones de vulnerabilidades en forma anual. Por ejemplo, el estándar PCI-DSS requiere que se hagan cuatro de estas evaluaciones en el año.

objetivo es promocionar y publicar contenido de seguridad y normalizar la transferencia de este 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 oficial es: **http://oval.mitre.org**.

Figura 2. **Sitio web del** Open Vulnerability and Assessment Language.

Penetration Test y ethical hacking

Si extendemos el concepto de Vulnerability Assessment y nos enfocamos en todos los procesos que involucren el manejo de la información de una organización, independientemente del medio en que esta se encuentre, nos acercamos a las evaluaciones del tipo **Penetration Test** o test de intrusión. A diferencia de los análisis de vulnerabilidades, estas pruebas no solo identifican las vulnerabilidades potenciales, sino que también tratan de explotarlas y, así, confirmar su existencia y el impacto real que podrían tener en la organización. Este punto es importante, ya que en muchas ocasiones, una vulnerabilidad reportada como crítica por el fabricante de la aplicación vulnerable no siempre es igualmente crítica en el contexto de una organización en particular. Puede darse el caso de que, incluso existiendo la vulnerabilidad, a partir de la presencia de otros controles compensatorios (recordemos otra vez el concepto de **defensa en profundidad**), la explotación de dicha vulnerabilidad se hace dificultosa o bien imposible. En esas situación, el riesgo que implica la presencia de la vulnerabilidad para esta organización puede no ser alto. Supongamos, por ejemplo, la existencia de una vulnerabilidad en un servidor de acceso remoto que, de ser explotada con éxito, permitiera tomar control total del equipo a distancia. Sin dudas, sería una vulnerabilidad crítica para cualquier organización.

Ahora complejicemos un poco el escenario. Imaginemos, además, que este servidor está en una red segmentada, a la cual solo se puede acceder desde otra red integrada únicamente por equipos de confianza. Además, el equipo que posee el servidor vulnerable tiene definido un conjunto de reglas de filtrado que únicamente permiten el acceso desde dos ubicaciones. Este ejemplo sencillo nos presenta un caso en el que tenemos una vulnerabilidad claramente crítica, ya que cualquier atacante podría tomar control del equipo en forma remota. Sin embargo, existe un conjunto de controles que dificultan en gran medida la explotación de esta vulnerabilidad: en nuestro caso, el doble

nivel de filtrado que debería pasar un atacante para poder explotar con éxito la vulnerabilidad.

Figura 3. **Sitio web del documento de la categoría Special Publications del Computer Security Division del NIST.**

De esta manera, vemos que resulta importante no solo verificar la posible existencia de vulnerabilidades, sino también evaluar cuál sería el impacto real para el negocio de la organización en caso de que fueran explotadas con éxito.

Hace unos años, un problema común que surgía al momento tanto de encarar un test de intrusión como de contratarlo era la falta de estandarización en cuanto a la metodología utilizada para llevarlo adelante y a las etapas en las cuales se dividía el proceso.

A partir de nuestra experiencia y la compartida con colegas, pero siempre apoyada en metodologías y estándares internacionales, hoy podemos dividir el proceso en cinco etapas conceptuales, las cuales desarrollaremos en los próximos dos capítulos:

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

Respecto a las metodologías, existen varias fuentes serias y confiables que marcan pautas y mejores prácticas sobre las cuales basar este tipo de evaluación, aunque en general, cada profesional puede incorporar sus variantes.

Algunos ejemplos pueden ser el documento denominado NIST Special Publication 800-115, del **National Institute of Standards and Technologies** de los Estados Unidos (**NIST**), el cual establece una guía de carácter técnico sobre cómo llevar adelante esta evaluación dentro de una organización. Por otro lado, también tenemos el **Open Source Security Testing Methodology Manual** (OSSTMM) de **ISECOM** y el **Information Systems Security Assessment Framework** (ISAFF) de **OISSG**.

MÁS VARIANTES

Desde la teoría estricta, existe una variante del análisis Black Box, conocida como Double Black Box o Double Blind, donde el cliente no tiene ningún conocimiento acerca de qué tipo de tests se harán, cómo se llevarán a cabo, ni cuándo.

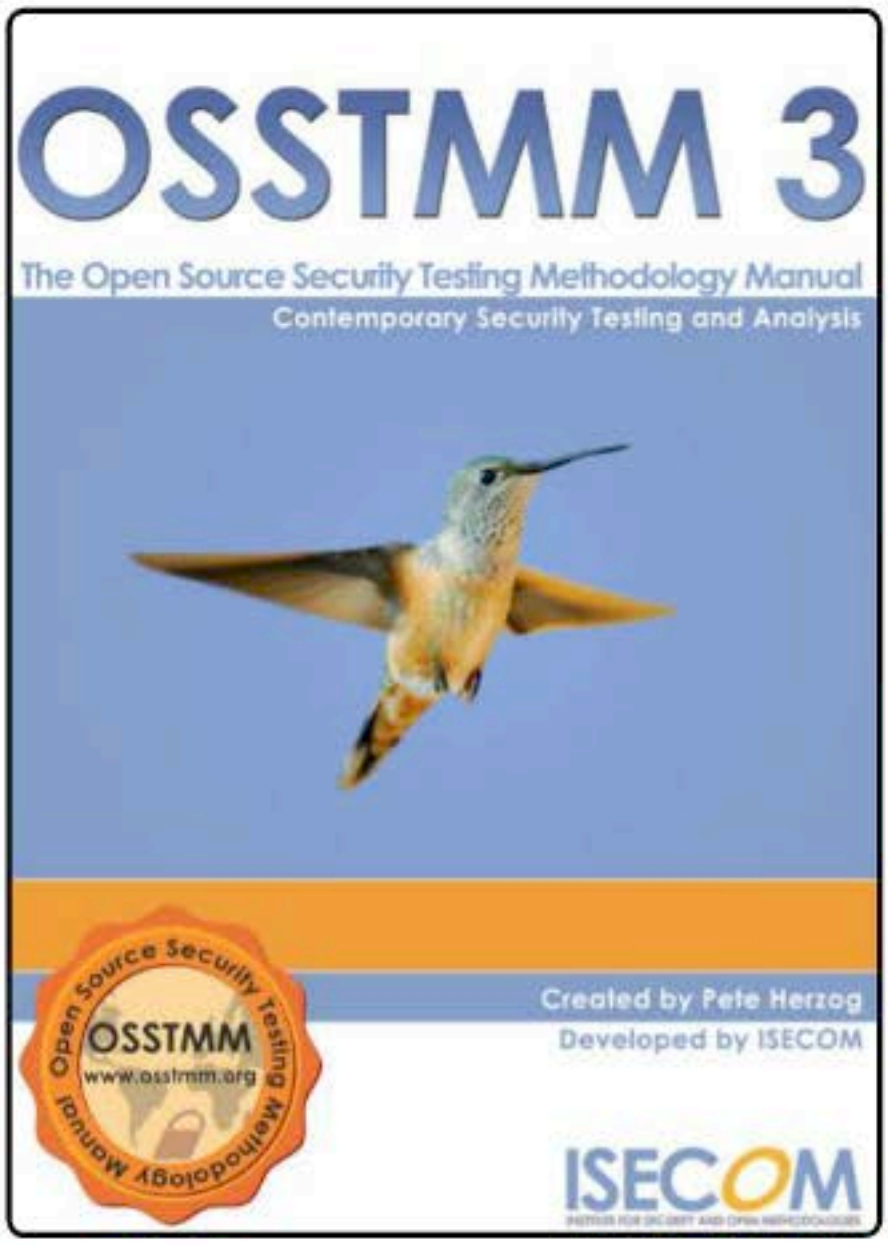


Figura 4. OSSTMM **es un manual sobre metodologías de evaluaciones de seguridad desarrollado por ISECOM.**

Análisis de brecha de cumplimiento

Otro tipo de evaluación que está creciendo en popularidad en estos últimos años es el **análisis de brecha** o **GAP Analysis**. Su objetivo es medir la diferencia entre la postura actual en seguridad de la información de una organización respecto a lo recomendado en algunos casos y lo exigido en otros por una determinada regulación o estándar. Si bien parece bastante sencillo en su definición, muchas veces no lo es debido a las particularidades de cada una de las organizaciones.

Mapping ISO 27001 Controls to PCI-DSS V1.2 Requirements

PCI-DSS V1.2 Requirement		ISO 27001 Control	
Build & Maintain Secure Network			
Requirement 1 – Install & Maintain Firewall Configuration to maintain data			
1.1	Establish firewall and router configuration standards that include the following:	A.10.6.1	Network Controls
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	A.10.1.2	Change Management
1.1.2	Current network diagram with all connections to cardholder data, including any wireless networks	A.10.6	Network Security Management
1.1.3	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	A.11.4.5	Segregation in networks
1.1.4	Description of groups, roles, and responsibilities for logical management of network components	A.11.4.1	Policy on use of network services
		A.11.4.7	Network routing control
1.1.5	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	A.10.1.1	Documented operating procedures
1.1.6	Requirement to review firewall and router rule sets at least every six months	A.10.6	Network Security Management
1.2	Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment	A.11.4.5	Segregation in networks
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment	A.11.4.5	Segregation in networks
1.2.2	Secure & synchronize router configuration files	A.10.6	Network Security Management
1.2.3	Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment	A.11.4.5	Segregation in networks
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment		
1.3.1	Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment	A.11.4.5	Segregation in networks

Figura 5. Mapeo del Requerimiento 1 PCI Build & Maintain a Secure Network **con los controles de ISO/IEC 27.001.**

Si bien es importante la verificación técnica por parte del profesional que lleva adelante la tarea o por algún colaborador, a fin de comprobar que lo relevado mediante entrevistas sea correcto, este paso no es usualmente requerido, ya que este tipo de evaluaciones suele basarse en la información que brinda la organización o que es relevada a partir de entrevistas.

A modo de complementar el punto anterior, es de gran utilidad realizar también una evaluación de vulnerabilidades o test de intrusión para poder verificar de manera técnica el cumplimiento de aquellos requisitos que están relacionados con los sistemas de información, las redes, etcétera. Esto, sin embargo, no es requisito para un análisis diferencial.

Figura 6. El sitio www.iso27000.es es un excelente recurso sobre la certificación ISO de seguridad.

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 estándares que existen, las empresas contratan servicios externos para realizar las evaluaciones de seguridad, en vez de hacerlo con personal propio? A continuación, iremos develando algunos de los puntos más importantes respecto a esta inquietud.

Por un lado, no todas las organizaciones poseen personal especializado que esté en condiciones de implementar esta clase de evaluaciones. En algunos casos, solo se cuenta con personal de sistemas o tecnología, que además realiza algunas tareas de seguridad solamente por ser el que sabe un poco más. Esta persona, por lo general, tiene conocimientos básicos en materia de seguridad de la información, por lo que sería impensado que pudiera llevar adelante un proyecto de evaluación de tal magnitud.

Clasificaciones de los tests

Según la forma en que realicemos las evaluaciones, surgirán diversas clasificaciones. Un criterio posible que tomaremos será en función de las herramientas que vamos a utilizar para llevar a cabo el proceso de evaluación de vulnerabilidades. Otra decisión se referirá al lugar desde donde se hará la evaluación: si es desde afuera de la organización o desde adentro. Finalmente, dependerá del alcance del análisis y hasta desde qué punto el cliente va a

¿ANÁLISIS DIFERENCIAL CONTRA QUIÉN?

Una entidad podría estar interesada en determinar cuál es la brecha que la separa del cumplimiento de diferentes normativas como ser PCI, ISO/IEC 27.001, Ley de Protección de Datos Personales o de una normativa de su banco central local.

conocer las tareas que implemente el analista. A continuación, analizaremos estos criterios y veremos todos los detalles de cada una de estas clasificaciones.

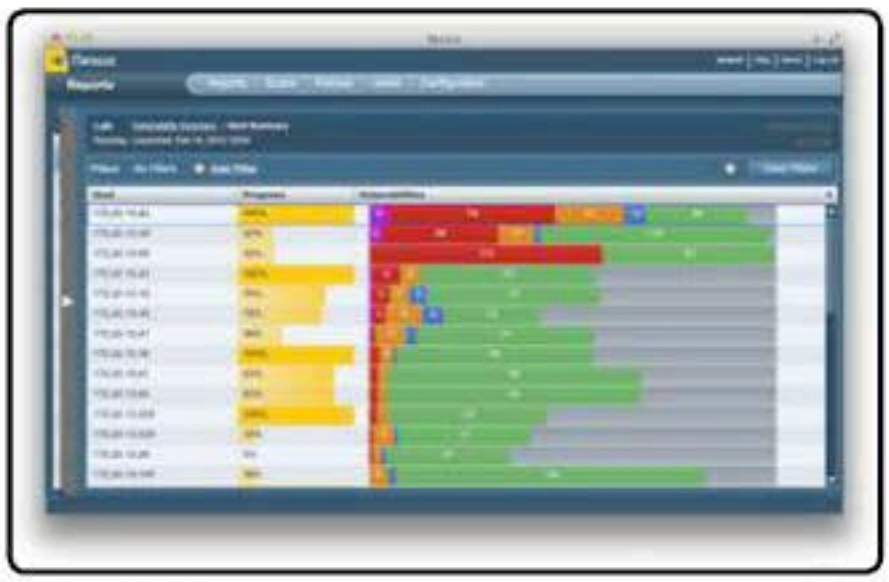


Figura 7. Las herramientas de escaneo como Nessus ofrecen completos reportes que ayudan a los analistas en sus informes.

Una primera distinción puede hacerse entre análisis del tipo manual o automatizado. Una parte importante del trabajo de análisis es realizado a partir de herramientas automatizadas. El escaneo de puertos, la exploración y búsqueda de vulnerabilidades y la explotación de vulnerabilidades, entre otras acciones, son realizados en gran medida a partir del uso de dichas herramientas. Algunas de ellas vienen preparadas para que, con una mínima configuración, se realicen todos estos análisis de manera rápida y con un buen porcentaje de efectividad, y un selecto grupo de ellas, además, al encontrar alguna vulnerabilidad, pueden llegar a explotarla. Una pregunta trivial que probablemente surja sería: ¿si existen tales herramientas, para qué está la figura del **Penetration Tester**?

Figura 8. El pentester cuenta con herramientas muy específicas para descubrir vulnerabilidades, como Acunetix, especializado en web.

La respuesta consta de varias partes. Por un lado, como veremos más adelante, un aspecto fundamental del proceso de evaluación de un Penetration Test es su informe de resultados. Usualmente se entregan dos: uno ejecutivo, orientado a la dirección o alta gerencia de la organización; y otro técnico, orientado al personal de tecnología de esta.

El profesional debe realmente comprobar, muchas veces en forma manual, la existencia real de las vulnerabilidades; y por otro lado, que debe volcar su experiencia en la interpretación de los resultados obtenidos por estas herramientas, identificando el riesgo que los hallazgos encontrados tengan en la organización.

Si bien estas herramientas efectúan una parte importante del trabajo y son esenciales para eso, lo que realmente aporta valor a dicha evaluación es el análisis que el profesional hace sobre toda la información, como si se tratara de un médico ante los estudios de un paciente.

Por otro lado, ciertos análisis necesariamente requieren la interacción de un profesional, ya que se deben tomar decisiones utilizando distintos criterios, la mayoría de ellos, basadas en la experiencia, momento a momento mientras se llevan a cabo las pruebas.

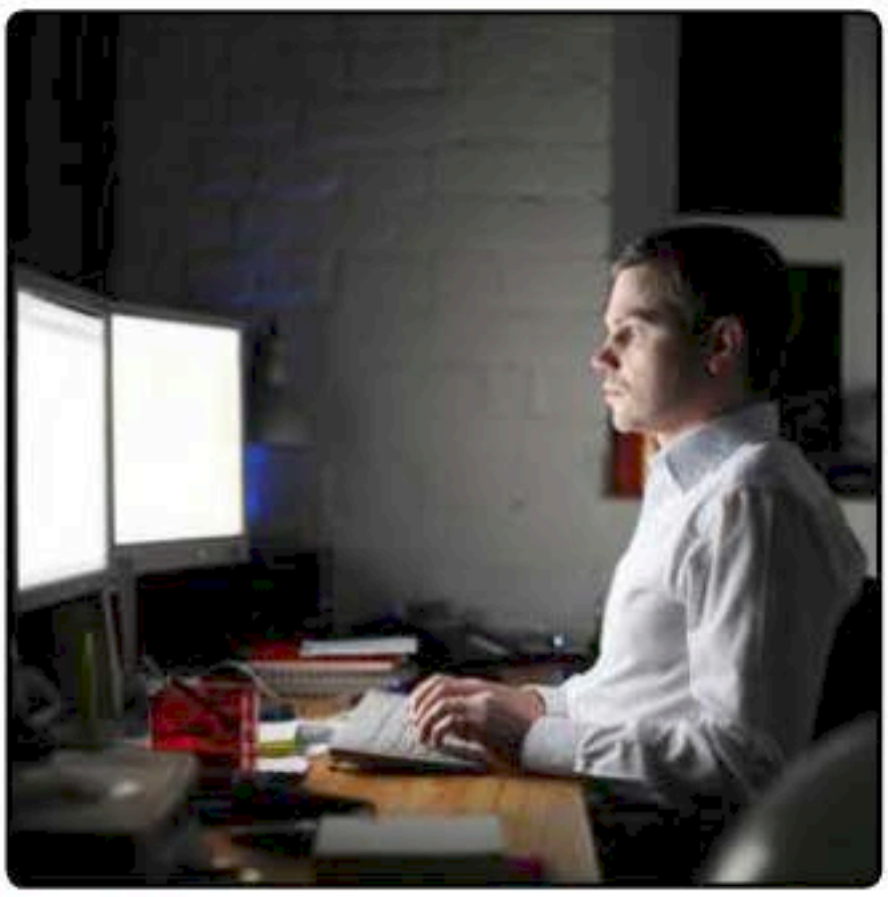


Figura 9. **Es común que un testeo del tipo White Box se realice desde adentro de la propia organización.**

Existe otra clasificación en el análisis que lo divide en externo o interno, y se refiere al contexto desde donde se hará la evaluación. Puede ser de manera externa, es decir que se realiza a distancia; o de manera interna, en cuyo caso el analista de seguridad efectúa las evaluaciones desde dentro de la organización. Por lo general, las evaluaciones de Penetration Test suelen contemplar ambos escenarios, aunque una vez más, esto dependerá de lo que se acuerde con el cliente.

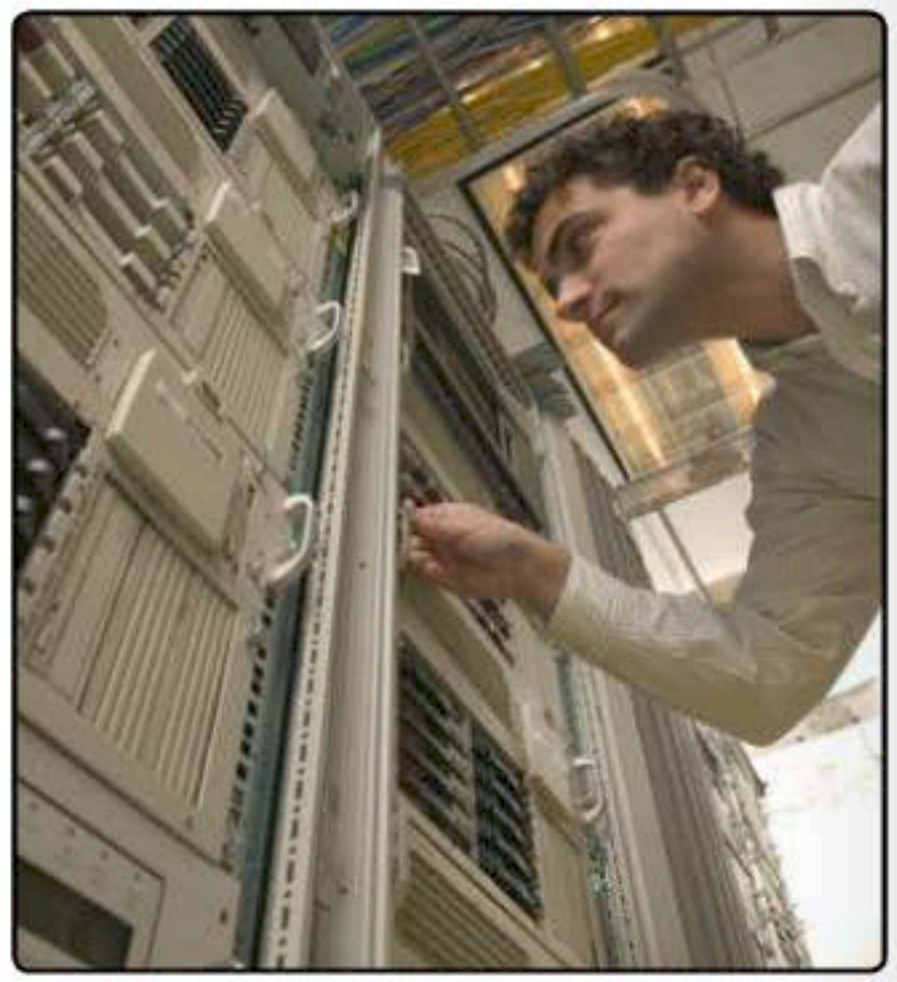


Figura 10. **En un testeo White Box, el analista conoce detalles internos de la infraestructura que estudiará.**

En el análisis interno, lo que se evalúa son todos aquellos puntos relacionados con la red interna y la información que circula en todos los niveles, no solo en formato digital. Desde adentro de la organización se llevan a cabo estos análisis, en los que los niveles de seguridad son diferentes de los que se encuentran definidos hacia fuera del perímetro de la empresa. En el caso del análisis externo, todas las pruebas se hacen en forma remota, buscando vulnerabilidades en la frontera, como, por ejemplo, en el firewall o en servidores que estén brindando servicios de Internet. En definitiva, se trata de hallar cualquier punto que, una vez explotado, permita obtener acceso a la DMZ o, mejor aún, a la red interna. Realizar ambos análisis permite auditar la efectividad de las medidas de acceso a distintos niveles.

Figura 11. **Previo a un testeo de seguridad se realiza un acuerdo de no divulgación, para que la información quede entre las partes.**

Como mencionamos en secciones anteriores, el test de intrusión simula en buena medida el proceso que lleva adelante un atacante real.

En función de esto, también es posible hacer una clasificación importante para determinar el alcance de la evaluación. Esto implica que, además de interno o externo, el test de intrusión puede ser según el nivel de conocimiento que se tiene sobre el sistema:

- White Box o definido
- Black Box o Blind
- Grey Box

En el primero de ellos, quien solicita el análisis provee a quien lo realiza información sobre la organización; por ejemplo, bloques de direcciones IP, credenciales de acceso, estructura de servidores, etcétera. Por otro lado, también se pacta el alcance de la evaluación, es decir, hasta qué punto se está permitido ingresar en los sistemas de la organización En este tipo de análisis, el cliente tiene total conocimiento de las tareas que realizará el analista de seguridad, del mismo modo que, muchas veces, también tiene información acerca de cómo y cuándo las hará, a pesar de que esto último no siempre es lo más recomendable.

Figura 12. **Muchos testeos comienzan por un relevamiento de requerimientos o análisis diferencial en forma de check list.**

LEY SARBANES-OXLEY

Conocida como SoX, es una ley de USA que monitorea empresas que cotizan en bolsa para evitar fraudes y riesgo de bancarrota. El cambio más representativo introducido es la responsabilidad de los directivos de las compañías en casos de fraude.

En el segundo caso, quien hace el análisis no recibe ningún tipo de información, con lo cual este examen simula de manera más realista el comportamiento que tendría un atacante real, y se lleva a cabo hasta donde las habilidades del especialista lo permitan.

En todos los casos que no sean extremos entre el desconocimiento absoluto de un sistema y el conocimiento total de sus detalles, estaremos hablando de un testeo del tipo Grey Box. En esta clase de pruebas, la persona que ejecuta el proceso tiene un conocimiento parcial de los detalles del sistema o de la infraestructura en general.

RESUMEN

En este capítulo tratamos las evaluaciones de seguridad y analizamos los distintos tipos de pruebas para conocer el estado de la seguridad en una organización. Encontramos diferencias entre una prueba técnica, un análisis complejo y un chequeo contra estándares. Finalmente clasificamos los tests para elegir el más adecuado.

Capítulo 3

Metodología de ethical hacking

En este capítulo analizaremos en detalle el proceso de ataque a un objetivo determinado.

RedUSERS.com

Fase de **reconocimiento**

A continuación, estudiaremos el proceso de ataque a un objetivo. La fase de reconocimiento es la que más tiempo insume dentro de la planificación de un ataque.

En esta primera etapa, el atacante busca definir el objetivo con el mayor nivel de detalle posible, y a partir de esto, obtener la mayor cantidad de información.

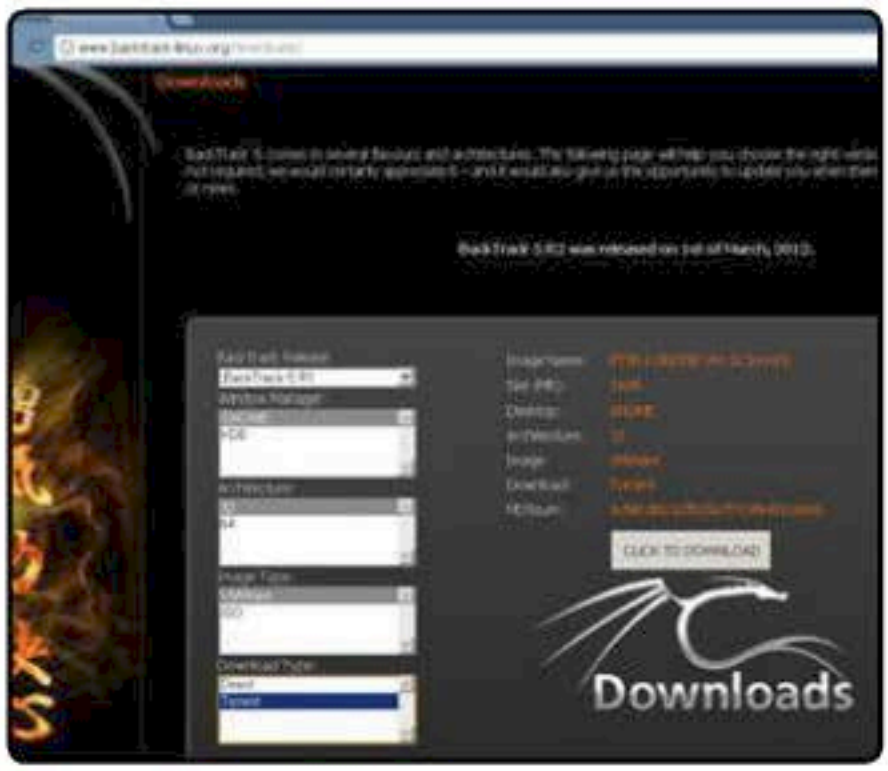


Figura 1. **Sitio de descarga de** Backtrack Linux **para el realizar pruebas de seguridad.**

Cuando nos centramos en las personas físicas, algunos ejemplos de información que podemos obtener de ellas son direcciones de correo electrónico, direcciones postales, información personal, etcétera. Desde la perspectiva corporativa, la información que se buscará obtener abarca direcciones **IP**, resolución de nombres **DNS**, y otros datos. En esta etapa, también denominada **Information Gathering** (**recopilación de información**), el atacante se basa en distintas técnicas para llevarla a cabo; las más utilizadas son **footprinting**, **ingeniería social** y **dumpster diving** o **trashing**.

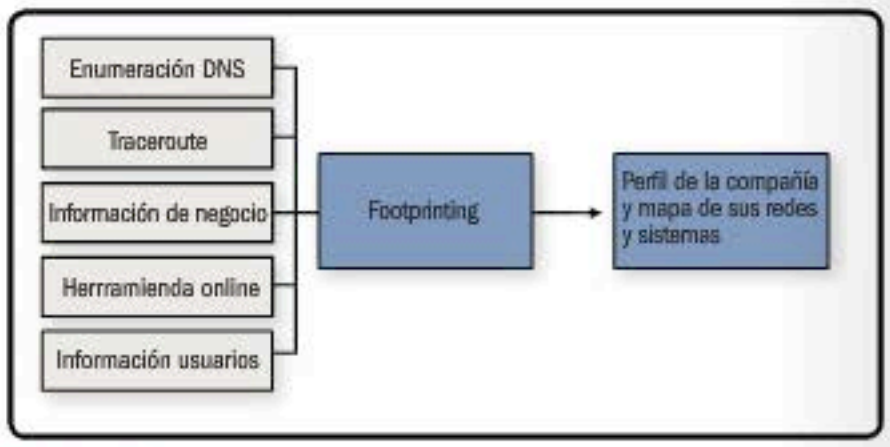


Figura 2. **Fase de footprinting como un proceso que toma entradas que da como resultado un perfil de la organización.**

Una herramienta fundamental son los buscadores como **Google**, **Bing**, **Yahoo** u otros específicos, y es imprescindible conocer las

TARGET OF EVALUATION

El Target-of-Evaluation es un sistema, producto o componente que se ha identificado como objeto de una evaluación o ataque. El concepto surge del estándar Common Criteria, que propone una serie de consideraciones al momento de adquirir un producto.

características avanzadas de búsqueda. Por otro lado existe una gran cantidad de recursos con **herramientas online** que permiten obtener información para usar en futuras fases.

Sabemos que debemos obtener toda la información posible relacionada con la organización, por lo que cuanta más información obtengamos, más posibilidades de lanzar un ataque exitoso tendremos. Actividades relacionadas con el negocio, organigrama y puestos de la organización, perfiles de usuarios, puestos que ocupan y hobbies son algunos de los datos que nos interesan.

A continuación veremos cómo llevar a la práctica estos conceptos, primero con el **footprinting de la red** exclusivamente (**Network Footprinting**) y, luego, con la recopilación de información sobre el negocio.

Una de las técnicas más utilizadas aquí es la enumeración **DNS** (**Domain Name System**), que tiene por objetivo ubicar todos los servidores DNS y sus registros dentro de una organización. Esta podría tener servidores DNS internos y externos, los cuales brindarían distintos tipos de datos del objetivo. Una herramienta que nos permite llevar adelante esta técnica es **Fierce**.

Figura 3. **Resultado de correr Fierce sobre el dominio** www.redusers.com.

Si un servidor está mal configurado, un atacante, sin utilizar ninguna herramienta más que las propias del sistema operativo (**dig** o **nslookup**), podría aprovechar esa configuración deficiente y copiar la lista completa de hosts.

GOOGLE HACKING

Este término fue popularizado por Johnny "j0hnny" Long, quien escribió los libros Google Hacking y No Tech Hacking y mantuvo por mucho tiempo la denominada Google Hacking Data Base (GHDB), encargada de almacenar información relacionada.

Figura 4. **Opciones de configuración del plugin** Social Friend Finder **donde se ven las redes sociales soportadas.**

Otra manera de relevar información relacionada son las consultas de **whois**, un protocolo TCP que realiza consultas a bases de datos whois para obtener información de carácter administrativo. A partir de whois podemos recopilar información de registro de un determinado dominio, como el nombre de la persona que realizó dicho registro, correo electrónico, número telefónico, direcciones IP de sus servidores, y su **ISP** (Internet Service Provider).

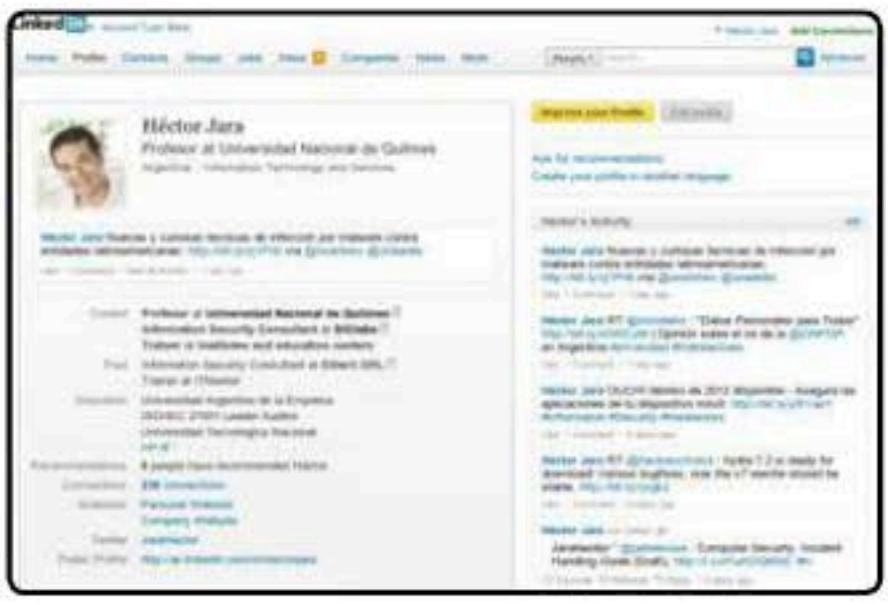


Figura 5. **Perfil en** LinkedIn. **Aquí obtenemos información asociada a compañías y sus empleados.**

Si nos enfocamos en el objetivo de esta etapa, queremos acercarnos lo más posible a armar un mapa de la red externa de una organización. Por lo tanto, más allá de conocer la existencia de determinados dispositivos asociados a su dirección IP, también sería interesante saber cuál es la disposición de estos. Por ejemplo, si la organización dispone de un router o un firewall, seguramente dichos dispositivos estarán en un nivel anterior a los servidores de correo, FTP, etc.

Figura 6. WorldIP **es un plugin de Firefox que muestra la dirección IP de un sitio y lanza comandos, como** `traceroute`, `ping` **y** `whois`.

La herramienta que nos permite obtener esa información se denomina **traceroute**, la cual dentifica el camino que sigue un determinado paquete desde un equipo de referencia (que puede ser el del atacante) hasta el objetivo. Así, en función del camino recorrido por el paquete, es posible obtener información adicional acerca de la configuración de red de la organización, por ejemplo, identificando routers, firewalls, etcétera.

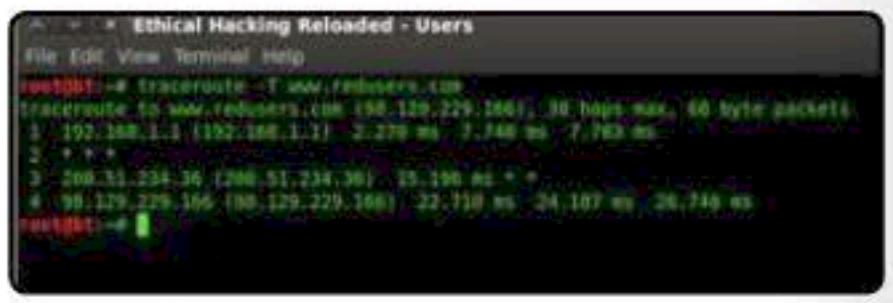


Figura 7. **Resultado de ejecutar** TCP traceroute **en el sitio** www.redusers.com.

Un atacante siempre deberá conocer las direcciones IP, ubicación geográfica y camino a través de Internet para llegar a su objetivo. Cada equipo encontrado en la ruta hacia él puede ser fuente de gran cantidad de información para futuros procesos. Una ventaja para los atacantes es que estas consultas pueden realizarse por medio de comandos específicos del sistema o a través de recursos online. En este último caso, existe la ventaja adicional de que la dirección IP que quedará registrada en los dispositivos de red de la organización no será la del atacante sino la del servicio.

Figura 8. Mediante el Google Dork "`Index of /" + passwd.txt` se obtiene información como la de esta imagen.

Entre la información que puede obtenerse en esta instancia, tenemos:

- Detección de sistemas específicos.
- Servidores publicados en Internet con vulnerabilidades específicas.
- Usuarios, contraseñas y demás datos sensibles expuestos al público.
- Correos electrónicos e información sobre usuarios para ataques de ingeniería social.
- Sitios de acceso a la administración de dispositivos.

Figura 9. Mediante BING Dork `ip: 98.129.229.166` se obtienen los sitios web asociados a dicha dirección IP.

A partir de la combinación de operadores de búsqueda, es posible hallar información relevante sobre una organización, que junto a otros datos obtenidos de otras fuentes y luego de un proceso de correlación y cruce, permite obtener información más elaborada desde el punto de vista del atacante. Así, este estaría en condiciones de lanzar ataques más sofisticados.

Figura 10. Resultado de la búsqueda del sitio www.redusers.com en www.archive.org.

También podemos hablar de búsqueda de **información offline**, con lo que por lo general nos referimos a todas aquellas técnicas que no están relacionadas directamente con el uso de la tecnología informática ni de Internet.

Las técnicas más conocidas en este caso son la **ingeniería social** y el **dumpster diving** o **trashing**, que consiste en buscar en los desechos de los cestos de papeles de las oficinas cualquier tipo de información que sea relevante para la etapa de recopilación.

Existen muchos casos en que se tiran papeles que contienen información confidencial en los cestos, sin pasarlos por trituradoras.

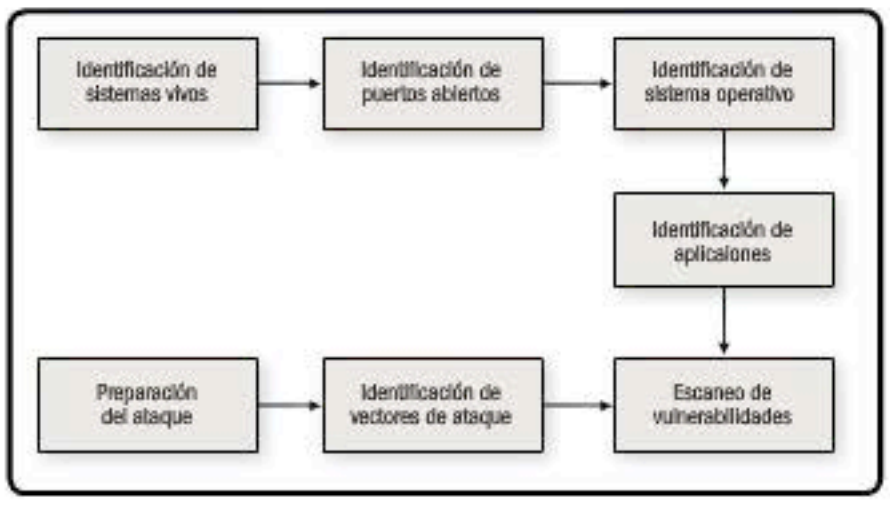


Figura 11. Metodología de escaneo: la salida obtenida en cada uno de los pasos alimenta al siguiente en la cadena.

Fase de **escaneo**

Hasta aquí hemos recopilado información del objetivo, tanto a nivel de red y de usuarios como la relacionada con el perfil de la organización. A partir de ahora, comienza la fase de escaneo, en la que analizamos el objetivo desde una perspectiva más técnica para detectar qué servicios y aplicaciones está ejecutando y qué vulnerabilidades pueden explotarse. Lo que se busca es encontrar posibles fallas, errores y vulnerabilidades de modo tal de definir los vectores de ataque de cara a que puedan ser explotados y ganar acceso al sistema.

Figura 12. PassiveRecon es un plugin de Firefox que permite centralizar el relevamiento de información.

Para el escaneo de puertos debemos comenzar por la primera herramienta de la caja: **NMAP**. Para

ESCÁNERES VARIOS

Si bien hay una amplia variedad de herramientas de escaneo de vulnerabilidades, como QualysGuard, SAINT y Nessus, este último es muy usado porque posee una licencia de uso personal y se puede descargar gratis para Linux, Windows y Mac OSX.

NMAP, un puerto puede presentar tres estados: **abierto**, **filtrado** o **cerrado**. El hecho de que un puerto esté abierto implica que el equipo objetivo acepta peticiones a él. Está filtrado cuando un firewall u otro dispositivo de red lo enmascara y previene que **NMAP** determine si está abierto o no.

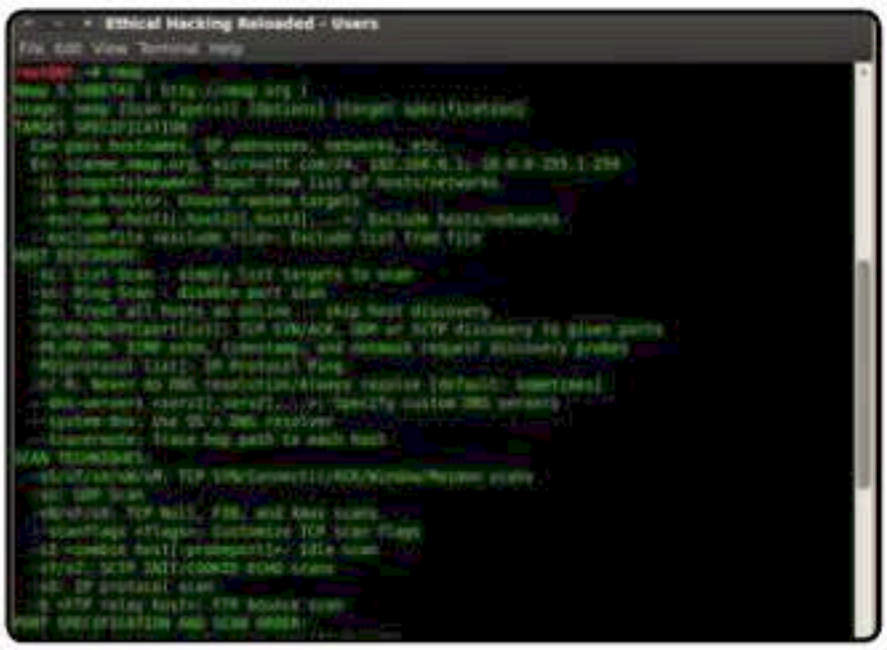


Figura 13. **Pantalla de NMAP con las distintas secciones que componen el manual de ayuda.**

Para verificar si un host se encuentra activo o no, utilizamos una herramienta que implementa la técnica de **ping sweep**. Esta consiste en enviar paquetes **ICMP request** (uno de los mensajes ICMP utilizados por el comando **ping**) a todos los hosts de una red. Si un host responde, implica que está online y es potencialmente un objetivo de ataque.

Una ventaja importante de esta técnica con respecto a otras es que sirve para enviar los paquetes en paralelo, es decir que toda la red será escaneada al mismo tiempo.

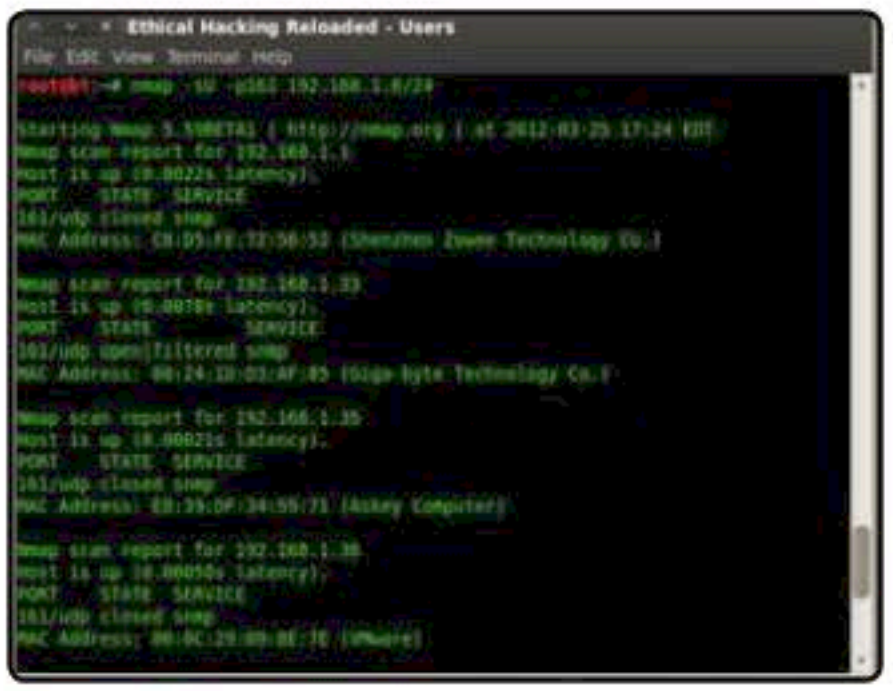


Figura 14. **Enumeración de dispositivos con SNMP habilitado en una red interna.**

Como segundo punto importante, la mayoría de las herramientas de escaneo incluye una opción de ping sweep. Como contrapartida, si un escaneo realizado solamente con esta técnica no detecta hosts vivos, no implica que estos no existan, ya que podría ser que el host escaneado simplemente no estuviera respondiendo el ping, con lo cual el resultado obtenido no reflejaría la realidad.

TRAZANDO RUTAS CON TCP

Si bien el funcionamiento original de las herramientas de traceroute está basado en el protocolo ICMP, existen implementaciones más modernas que utilizan TCP, y también existen algunas herramientas que presentan resultados gráficos.

Figura 15. Resultado de lanzar un ping sweep a la red de clase C 192.168.1.0/24.

El escáner utiliza técnicas basadas en el protocolo TCP, las cuales surgen de la activación de uno o varios de sus flags. La manera más sencilla de identificar el estado de un puerto es tratando de conectarse a él. Si el puerto se encuentra abierto responderá un ACK; en cambio, si está cerrado, responderá un RST; en tanto que si está filtrado, no se recibirá ninguna clase de respuesta. En caso de que el puerto esté abierto, continuamos con los otros dos pasos y establecemos la conexión. Este escaneo es conocido como **TCP Connect**.

Figura 16. Captura de pantalla de una cámara IP publicada a Internet, con un usuario y una contraseña por defecto.

Si bien esta forma es válida, desde el punto de vista del atacante es muy ruidosa, porque deja muchos registros y es fácilmente detectable. Por eso existe una variante: **SYN Scan**, cuya diferencia es que en vez de responder el último paso con un paquete ACK, envía un RST de modo tal de cortar la conexión. Este escaneo deja menor cantidad de registros en el objetivo. Además de estos, existe una serie de otros escaneos implementados por **NMAP** para funciones específicas.

Figura 17. En este banner encontramos información relevante, el servidor **(Apache), la** versión **(2.2.17) y el** SO **(Linux, Ubuntu).**

Otro proceso es el de **OS fingerprinting** que tiene por objetivo detectar cuál es el sistema operativo del equipo escaneado. Puede llevarse a cabo en forma pasiva o activa. Se dice que la detección es pasiva cuando el análisis se realiza solo en función de los paquetes que el host objetivo envía; es decir, quien está escaneando únicamente captura paquetes enviados por el objetivo a través de la red y los analiza para intentar descubrir patrones que permitan identificar el sistema operativo. La herramienta **P0f**

hace este tipo de detección. En el caso de la identificación activa, el host que está escaneando envía paquetes armados especialmente de modo de evaluar la respuesta. Si bien es más efectivo, es menos discreto.

Figura 18. **Resultado de un escaneo de puertos junto con la detección del sistema operativo al host** 192.168.1.55.

Una vez que identificamos los puertos abiertos, como regla general podemos asociar a cada uno un servicio en especial. A partir de la detección del sistema operativo también podemos inferir qué aplicaciones se están ejecutando en dicho equipo. Una técnica más precisa utilizada para la detección de aplicaciones es la de **Banner Grabbing**. Dado que la mayoría de los servicios poseen algún banner que los identifica, si nos conectamos al servicio, tal vez podamos obtenerlo.

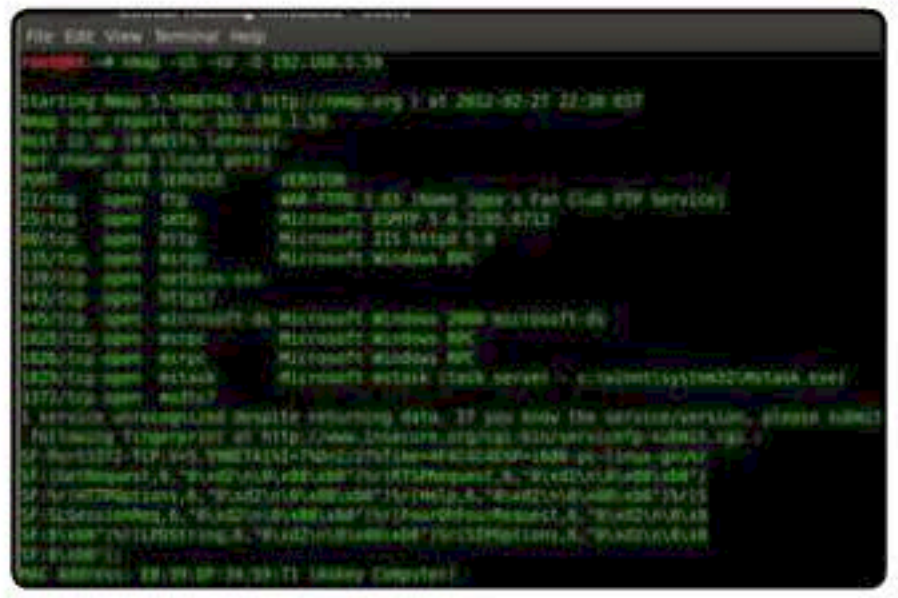


Figura 19. **Identificación de puertos abiertos, SO utilizado y aplicaciones con sus versiones.**

A partir del escaneo de puertos, necesitaremos contar con otras aplicaciones denominadas escáneres de vulnerabilidades, que se encargan de identificar vulnerabilidades conocidas, en base a un conjunto de **plugins**. Cuando una vulnerabilidad nueva es reportada, se genera un nuevo plugin que permite identificarla y se agrega a la base de datos, una vez actualizada. Estas herramientas utilizan la arquitectura cliente/servidor, por medio de la cual varios equipos pueden conectarse a un servidor y lanzar escaneos, pero manteniendo una única base de datos de plugins.

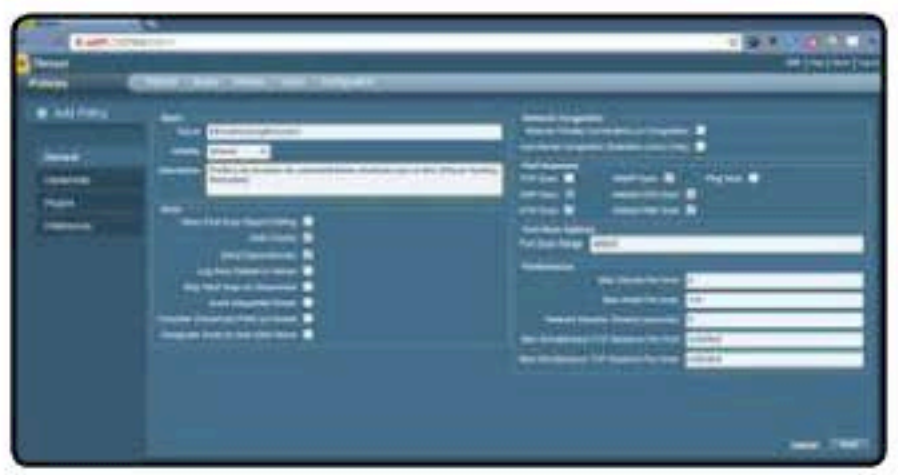


Figura 20. **Extracto de la página de inicio. Las opciones principales son `Reports`, `Scans`, `Policies`, `Users` y `Configurations`.**

Una vez que el escáner analiza las posibles vulnerabilidades, el siguiente paso es definir cuáles serán los **vectores de ataque** que se emplearán. Se denomina vectores de ataque a todos los posibles caminos para lanzar un ataque en función de las vulnerabilidades detectadas.

Antes de lanzar el ataque, el ejecutante toma todas las medidas necesarias para dificultar en la mayor medida posible su identificación, buscando el **anonimato** en la red. Para lograrlo, uno de los recaudos tomados es el uso de **servidores proxy** como intermediarios entre él y el objetivo.

Una alternativa también válida para lograr discreción en la Web son los denominados **anonymizers**, servicios que buscan volver anónima la navegación utilizando un sitio web que actúa como proxy para el cliente web y remueve información de identificación mientras se navega. Otra alternativa es el uso de la red **TOR**, que si bien es muy efectiva, puede ralentizar las velocidades.

Cómo podemos notar existe una gran variedad de técnicas y herramientas que se pueden implementar en la fase de escaneo.

Figura 21. **Página inicial del sitio del proyecto TOR**: www.torproject.org.

Fase de **enumeración**

Si bien es posible enumerar dispositivos y recursos externamente, la **fase de enumeración** se realiza desde la red interna, ya sea porque se trata de un test de intrusión interno o bien porque se realiza mediante la explotación de un vector de ataque, como un **ClientSide** (del lado del cliente).

El objetivo principal es obtener la mayor cantidad de información de la red interna que nos permita lanzar ataques más elaborados. Los nombres o IDs de usuarios, los grupos de

LA FOCA

Para realizar tareas de reconocimiento y relevamiento de información de sistemas y metadatos, podemos descargar de manera gratuita la herramienta FOCA desde el enlace www.informatica64.com/foca.aspx, dejando nuestro correo electrónico.

dominio, los nombres de equipos, los recursos compartidos y los servicios brindados internamente son solo algunos de los objetivos puntuales de esta etapa.

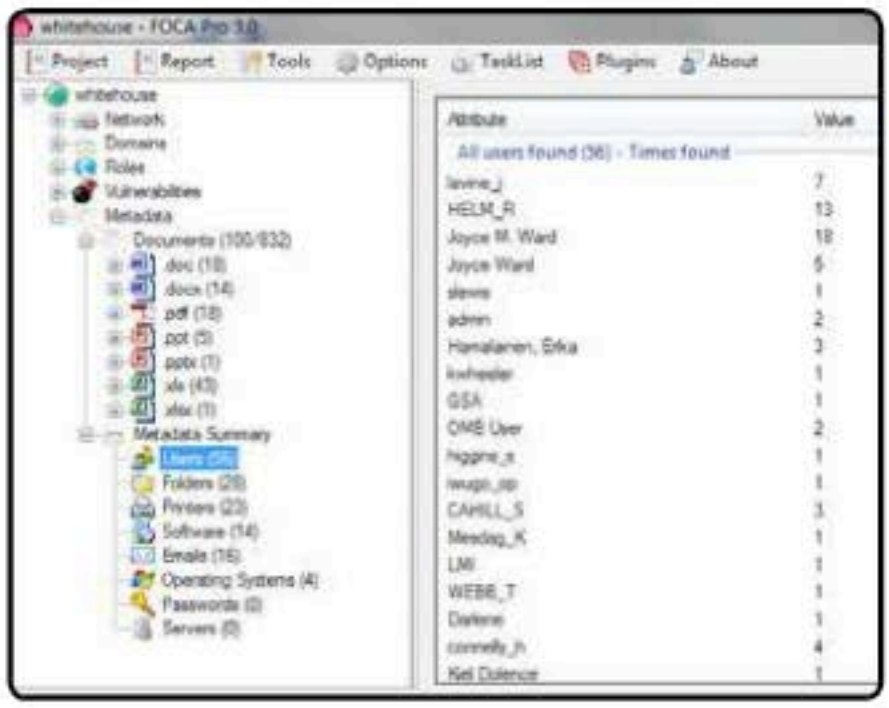


Figura 22. Resumen de la información recopilada mediante el análisis de los metadatos de archivos en el sitio con la herramienta FOCA.

De la misma manera que en la etapa de reconocimiento inicial, la obtención de banners de servicios, en forma ya sea manual o automatizada, es una buena fuente de información. El uso de comandos de Windows, la enumeración de usuarios por fuerza bruta y el uso del protocolo **SNMP** también son medios que brindan información relevante.

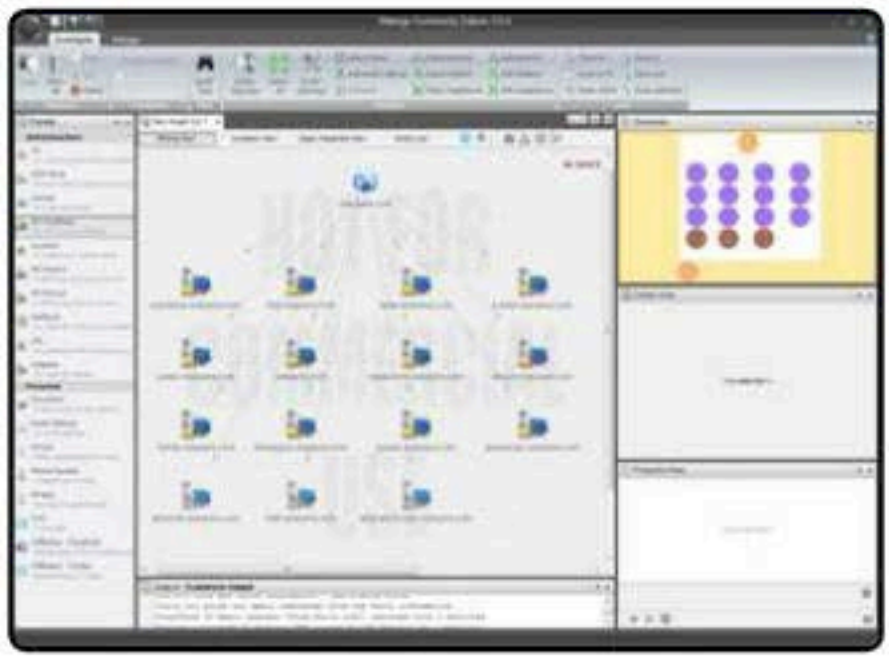


Figura 23. Información de un dominio encontrada con la herramienta Maltego, utilizada para relevamiento.

En el caso de los sistemas Windows, dentro del directorio **`Support/Tools`** hay una gran variedad de herramientas, muchas de las cuales pueden usarse para realizar la enumeración de sistemas. Si somos parte del dominio, podemos consultar información con comandos **`net`**.

Con esta información sabremos a qué usuarios nos convendría **impersonar** para poder tomar control de la red. Sobre todo es interesante también conocer cuál es el nombre de los distintos equipos, ya que la nomenclatura, por lo general, puede orientarnos respecto a la función que estos cumplen.

METADATOS

Los metadatos son datos abstractos que sirven para definir a otros datos con mayor nivel de especificidad. Algunos ejemplos de metadatos son las cabeceras de los distintos formatos de archivos como por ejemplo DOC, PDF, JPEG **y** XLS.

Además de los usuarios y los equipos, la enumeración de recursos compartidos cobra especial importancia ya que es muy frecuente encontrar carpetas, impresoras, unidades de red y demás recursos de toda clase, que no tienen implementado un control de acceso que resulte eficiente.

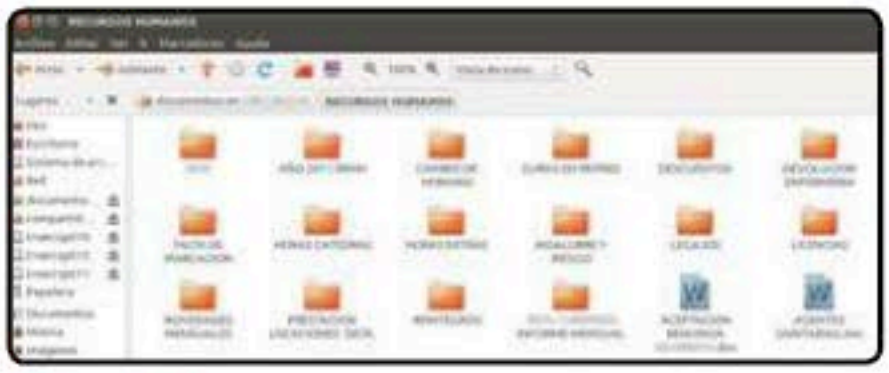


Figura 24. **Ejemplo de una carpeta con información de recursos humanos accesible desde la red interna.**

Debemos saber que la enumeración de recursos puede realizarse mediante la implementación de una gran variedad de técnicas.

Entre estas, por lo general, las más utilizadas son las que se efectúan a través de **NETBIOS**, la **enumeración DNS** o la **transferencia de zonas**, cuando es posible, o bien mediante el protocolo **SNMP** (Simple Network Management Protocol).

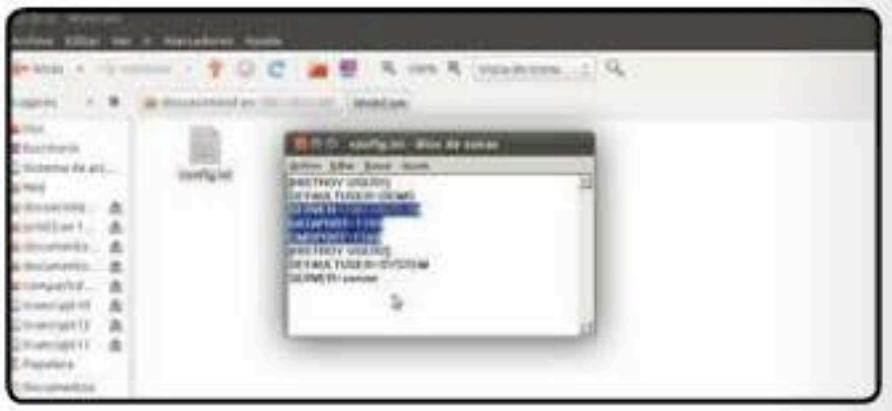


Figura 25. **Tenemos un ejemplo de un archivo de configuración de un servidor de un sistema de cámaras de vigilancia.**

Adicionalmente, es valioso conocer las aplicaciones que posee la organización. De manera análoga a la identificación de aplicaciones externas, también podemos conectarnos a los servicios para obtener detalles, para lo que podemos utilizar herramientas como **telnet** o **netcat**.

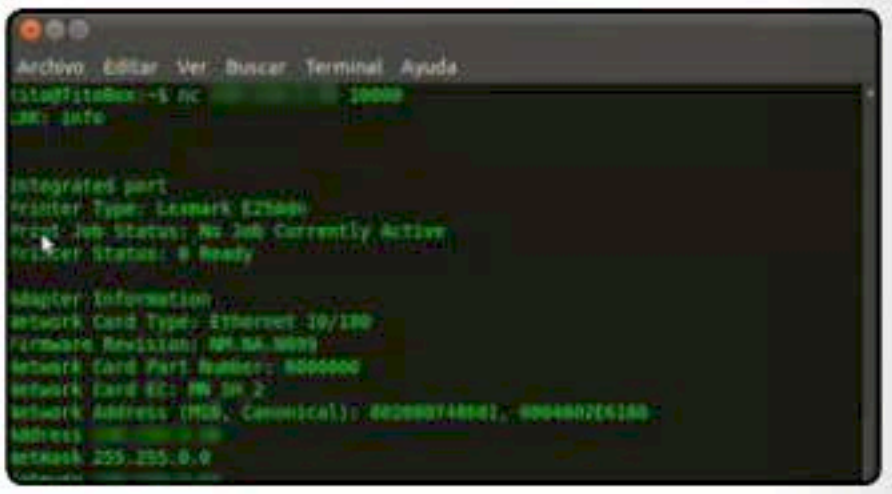


Figura 26. **Enumeración de una impresora. Mediante el comando** nc, **nos conectamos al puerto de configuración.**

SYSINTERNALS

En 1996, Mark Russinovich y Bryce Cogswell crearon un set de herramientas para Windows llamado SysInternals. Luego de diez años, Microsoft compró la empresa y ha seguido manteniendo dicho set, que incluye herramientas de administración y diagnóstico.

Por otro lado, también es posible lanzar escaneos con credenciales o del tipo **caja blanca**. Esto es a partir de las credenciales de un usuario de dominio, se puede ingresar al sistema en cuestión y realizar un análisis del equipo con mayor nivel de detalle, ya que se puede acceder a información interna del equipo y así conocer todas las aplicaciones que se encuentran instaladas. Con esto, independientemente de las vulnerabilidades, también podremos conseguir un listado de todas las aplicaciones instaladass.

En el caso puntual de los sistemas Windows, esta información se puede obtener mediante el registro del sistema.

Figura 27. **Escaneo de vulnerabilidades realizado con** QualysGuard.

Además de los recursos internos, también es de gran utilidad conocer los dispositivos de la red interna, como, por ejemplo, firewalls, routers, módems y otros equipos específicos.

Una de las técnicas más usadas para relevar estos recursos es la enumeración **SNMP** mencionada previamente, ya que el protocolo es utilizado para gestionar remotamente dispositivos, desde equipos de red y servidores, hasta **UPS** (Uninterruptible Power Supply).

En este caso, otro protocolo que, por sus características, puede ser implementado para la enumeración de los dispositivo es **uPnP** (Universal Plug and Play), el cual permite que los dispositivos que lo soportan tengan la posibilidad de modificar sus propias configuraciones de manera automática cuando reciben una petición específica.

Figura 28. **Enumeración de dispositivos mediante Universal Plug-n-Play con la herramienta** `miranda`.

FOUNDSTONE

Foundstone Inc. es una empresa fundada en 1999 que ofrecía software, dispositivos, servicios de consultoría y educación. Su presidente era George Kurtz, autor del legendario libro Hacking Exposed. En el año 2004, la firma fue adquirida por McAfee.

Fase de ingreso **al sistema**

A partir de la información recopilada y teniendo en cuenta las vulnerabilidades detectadas, aquellas que tengan disponible mejores **exploits** o cuya explotación sea más sencilla serán las elegidas y priorizadas al momento de lanzar el ataque, de forma tal de maximizar las probabilidades de éxito. Algunos vectores de ataque típicos pueden ser los de denegación de servicio, los ataques contra una aplicación web, la fuerza bruta a un formulario de login y la ingeniería social, entre otras.

El término **exploit** en informática se refiere a una **pieza de software, fragmento de datos** o **secuencia de comandos** que aprovecha un error, falla o debilidad, a fin de causar un comportamiento no deseado en un sistema o aplicación, pudiendo forzar cambios en su flujo de ejecución con posibilidad de ser controlados a voluntad.

Figura 29. **Sitio de CVSS con su última versión publicada.**

Es importante comprender las diferencias entre los siguientes tipos de exploits:

- **Exploits remotos:** pueden ser lanzados desde una ubicación diferente de la del equipo considerado víctima
- **Exploits locales**: son ejecutados localmente en el equipo y, en general, permiten elevar ciertos privilegios.

A medida que el estudio de vulnerabilidades fue creciendo, la evolución de su explotación atravesó un largo camino desde la forma manual tradicional hasta los **frameworks** modernos, que ofrecen innumerables posibilidades para realizar las mismas tareas que años antes demoraban mucho más tiempo. Estos permiten la **reutilización del código**, la **estandarización** de los exploits y, por sobre todas las cosas, la **simplificación del proceso** de ataque. En la actualidad, existen diversos frameworks de explotación, como **Immunity Canvas, Core Impact** y **Rapid7 Metasploit**.

Figura 30. **Buscador de exploits y módulos auxiliares en el sitio** www.metasploit.com/modules/auxiliary.

Un ataque externo, en caso de ser exitoso, finalizará con un acceso que permita tomar acciones desde el interior de un sistema, idealmente, dentro de la red interna. Cuando un atacante

obtiene acceso muchas veces es con credenciales de usuario restringido, ya que, como sabemos, suele ser más sencillo vulnerar a un usuario común que al administrador, con lo cual deberá elevar dichos privilegios. Para esto, lanza un exploit local luego de haber comprobado que era vulnerable, y si todo sale bien obtiene el nivel deseado. La elevación de privilegios puede ser de tipo vertical u horizontal. La primera consiste en obtener privilegios de nivel superior a los que se tiene, y la segunda se refiere a la posibilidad de acceder a otras cuentas de usuario del mismo nivel de acceso.

Una vez obtenido el acceso, se deseará ejecutar comandos y correr aplicaciones en el sistema. El requisito es haber establecido un canal entre el sistema remoto y el del atacante, lo cual puede hacerse a partir de cualquier protocolo (HTTP, SMTP, ICMP, etcétera).

Finalmente, se deberá contar con un elemento que permita dicha comunicación, ejecutándose en el objetivo. Muchas aplicaciones y comandos permiten pasar **parámetros de ejecución remota**, por lo que pueden aprovecharse para esta fase, y si no, tal vez sea preciso obtener directamente una consola en la cual ingresar los comandos propios del sistema objetivo (no necesariamente una consola del sistema operativo). En sistemas Windows puede utilizarse **PsExec** o **Remoxec**, que ejecutan comandos empleando servicios **RPC Task Scheduler** o **DCOM Windows Management Instrumentation**.

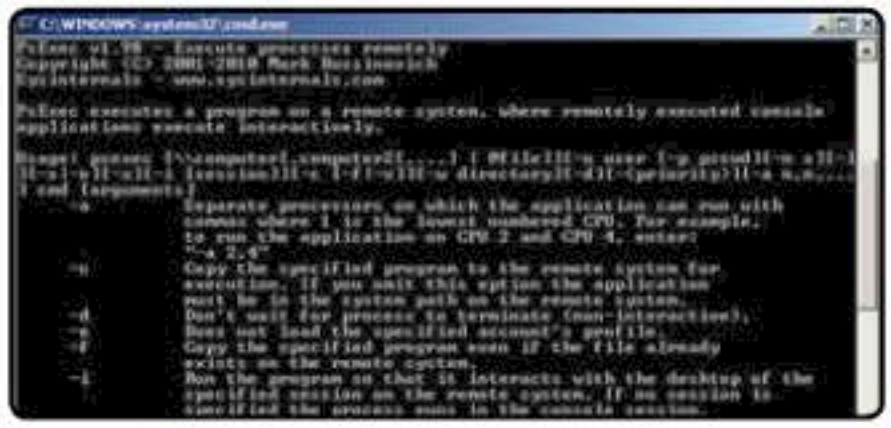


Figura 31. PsExec **permite ejecutar comandos en forma remota.**

Fase de mantenimiento del acceso

Podríamos creer que una vez que un atacante toma control sobre un sistema y accede a él, su tarea ya está cumplida. Sin embargo, por lo general el acceso es solo un paso para la

EXPLOITS CLASIFICADOS

Podemos clasificar los exploits según diferentes criterios: la forma en que este afecta al sistema objetivo (local o remoto) el tipo de vulnerabilidad que explota (stack overflow, heap overflow, etc.), y la clase de ataque (DoS, ejecución de código, etc.)

consolidación de la posición, que constituye el verdadero objetivo.

Una de las formas de mantener el acceso es utilizando **malware** (malicious software) que implica todo tipo de código malicioso, no solo virus. Un malware no es más que una pieza de software diseñada para infectar un sistema, y se trata de componentes desarrollados con el objeto de concretar alguna acción maliciosa. Su peligrosidad se establece sobre la base de dos criterios principales: la capacidad de daño y la posibilidad de propagación.

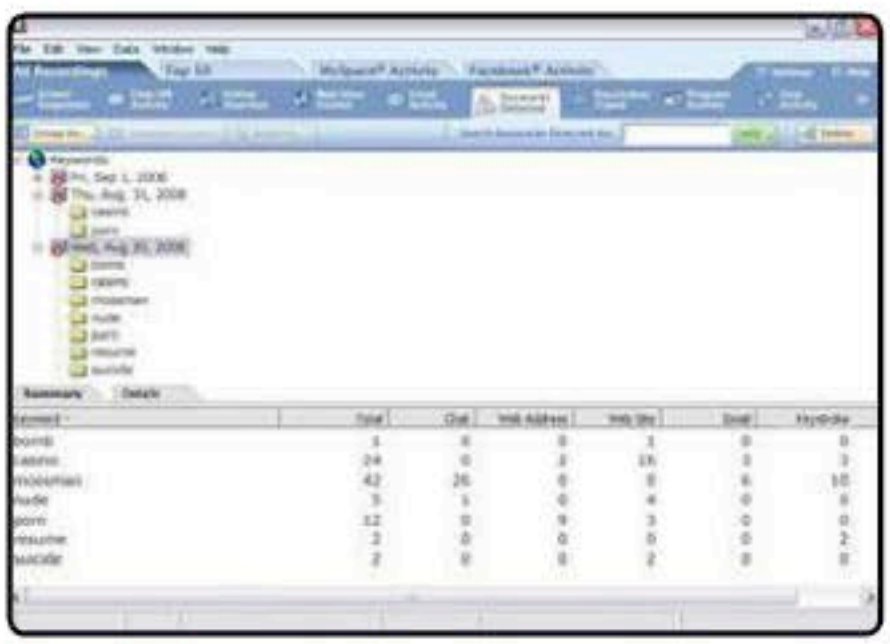


Figura 32. Keylogger Spector **cuenta con una poderosa función de detección de palabras.**

La clasificación actual del malware por la forma de propagación, incluye: **troyanos, gusanos, adware, spyware**, y **virus** propiamente dicho. Además, considerando sus acciones o características, aparecen los **keyloggers, backdoors, ransomware, rogue** y **rootkits**.

Vale destacar el comportamiento de los gusanos, que no necesitan infectar a otros archivos para multiplicarse porque aprovechan las vulnerabilidades existentes en un sistema para realizar su propagación.

Entre las aplicaciones que más se utilizan por su funcionalidad en un ataque están los **keyloggers**, destinadas a grabar todo lo escrito por teclado (aunque la mayoría no solo se remite a esto) para luego enviarlo al atacante o almacenarlo a la espera de ser recuperado. Si bien su principal implementación es en software, existen dispositivos de hardware que ofrecen las mismas funcionalidades, colocándose a modo de adaptador entre el teclado y el conector del motherboard, y almacenando directamente la información en una memoria interna.

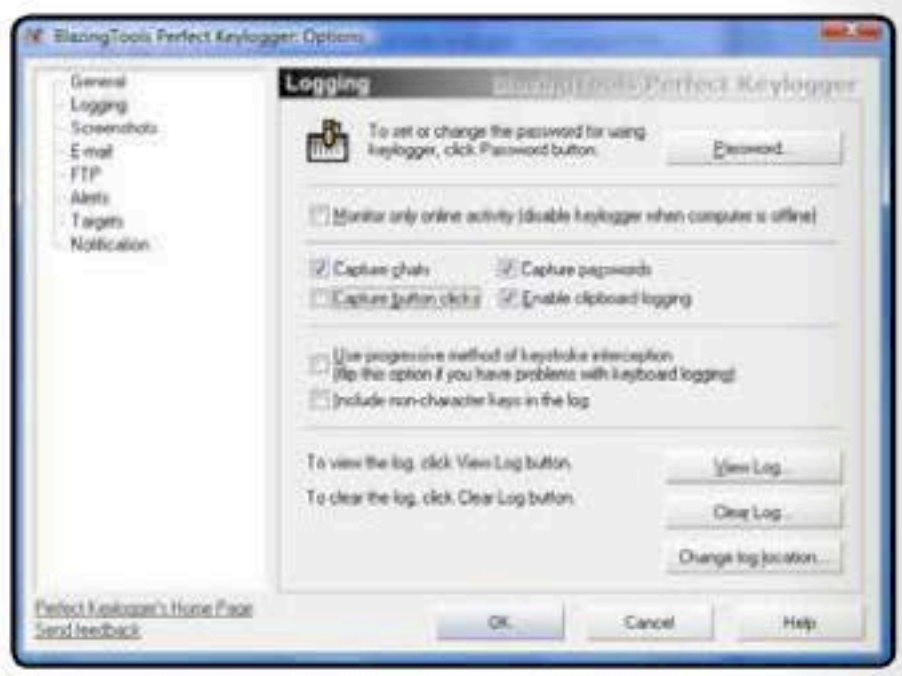


Figura 33. Perfect Keylogger **ofrece una gran cantidad de interesantes opciones, como, por ejemplo, la captura de pantallas.**

En cuanto a los troyanos, son programas que llevan oculta una funcionalidad que será usada con fines maliciosos (la palabra hace referencia al **Caballo de Troya**). Una de las

principales diferencias con un **virus** es su incapacidad para replicarse. Si bien un troyano no necesariamente debe funcionar como puerta trasera, la mayoría lo hace; por lo tanto, nos referimos a troyanos teniendo en mente su aplicación como herramienta de administración remota. Suele llegar al sistema como un programa aparentemente inofensivo, pretendiendo ser algo que no es o hacer algo que no hace. A veces, como adjuntos de correo o como parte de una aplicación "troyanizada". También hay malware que introduce troyanos y keyloggers como parte de su accionar (**downloaders**).

Figura 34. **Configuración de** Invisible Keylogger, **uno de los más elegidos para la captura de teclas en sistemas Windows.**

Como los sistemas actuales están muy estandarizados, sus componentes, archivos y comandos suelen ser los mismos entre instalaciones. Esto llevó al desarrollo de los **rootkits**, que aprovechan las herramientas de los sistemas en su contra, alterando su funcionamiento.

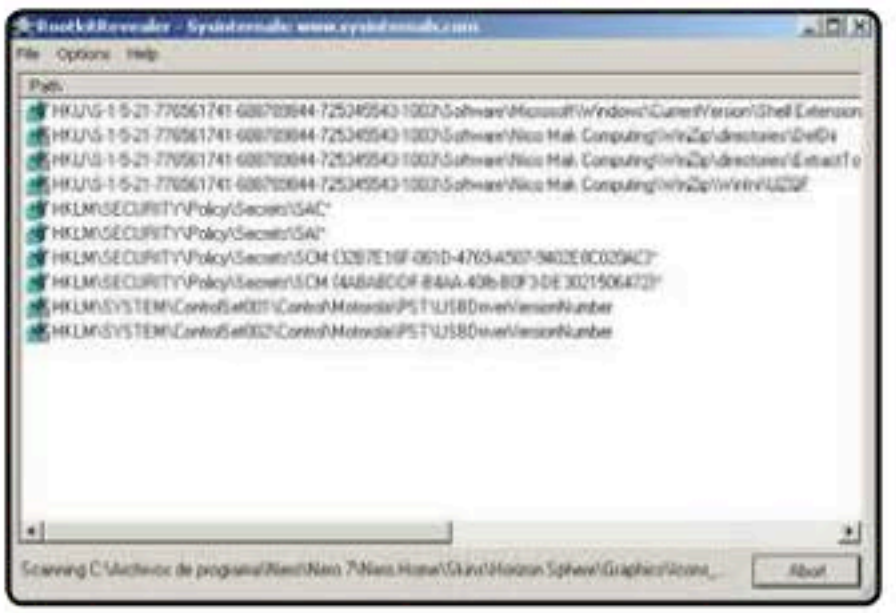


Figura 35. **El detector** Rootkit Revaler **es un clásico de** Sysinternals, **se destaca por su simpleza y efectividad.**

Entonces, podemos decir que un rootkit es una herramienta o un conjunto de ellas cuya finalidad es esconderse a sí misma y a otros programas, procesos, archivos, directorios, registros y puertos para permitir mantener acceso a un sistema. En sus orígenes, hacía referencia a un grupo de herramientas recompiladas de

EL SALÓN DE LA FAMA

Los virus, así como las estrellas de Hollywood, tienen su salón de la fama. La lista incluye sin dudas a: Melissa, CIH (Chernobyl), Love Bug (I Love You), Sircam, Nimda, Código Rojo, SQL Slammer, Blaster, Klez, Nicehello, Bugbear, Sobig y Sasser

UNIX, que habiendo sido modificadas ocultaban actividades maliciosas, con lo que un intruso podía mantener el control de un sistema con privilegios de **root**, oculto a administradores. En general, podemos clasificarlos en dos grandes grupos: los que van integrados en el núcleo y los que funcionan a nivel de aplicaciones.

Figura 36. **El antispyware Ad-Aware es uno de los más populares y cuenta con una versión gratuita muy completa.**

Más allá del malware, una acción que puede desear el atacante al penetrar un sistema es ocultar los archivos, ya sea para encontrarlos cuando regrese, transmitirlos de manera sigilosa utilizando el sistema como canal oculto o también y más comúnmente, para que todo lo que se haya creado, descargado y generado localmente permanezca a salvo de los ojos detectores del sistema operativo y del software de seguridad implementado.

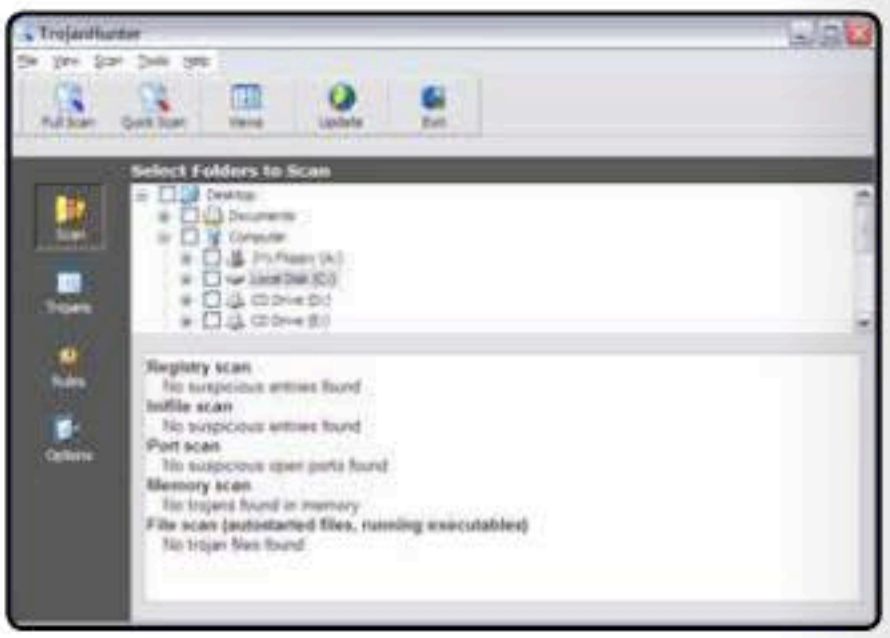


Figura 37. Trojan Hunter **es uno de los antitroyanos más elegidos, tiene una interfaz muy intuitiva.**

Dos métodos muy empleados para hacerlo son la esteganografía y el uso de las características avanzadas de los sistemas de archivos, como los **ADS** (Alternate Data Streams).

Desde una perspectiva formal, diríamos que la esteganografía es la disciplina que se ocupa de estudiar las estructuras de mensajes como

ATAQUES CLIENTSIDE

En este tipo de ataques se requiere la intervención del usuario del lado cliente, y es asincrónico, porque el momento en que se lanza no es el mismo en que se obtiene el acceso. Además, es un ataque que se lanza a ciegas.

objeto matemático, con el propósito de ocultarlos dentro de otros.

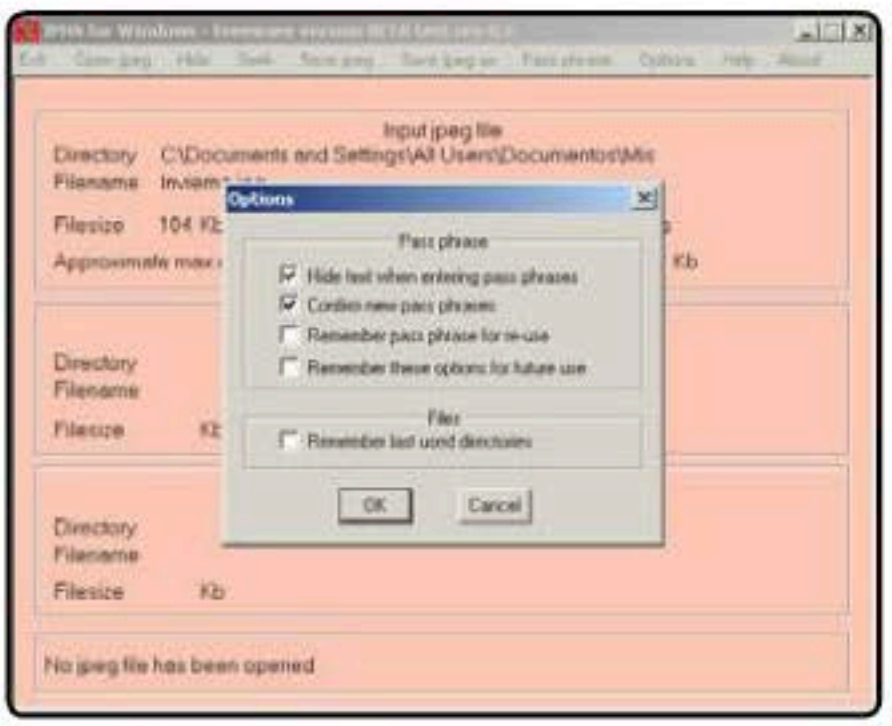


Figura 38. Opciones de JP hide and seek, que permite ocultar información en archivos JPEG.

Los ADS son una característica del sistema de archivos **NTFS**, que suele usarse para mantener información asociada a un determinado archivo o directorio. Cualquier usuario del sistema puede, por defecto, utilizar esta característica tan solo teniendo permiso de escritura.

Una limitación que encontramos, en principio, es la de enviar un archivo por Internet, ya que no se manda el stream alternativo, sino solo el principal. Sin embargo, si utilizamos la herramienta **Backup de Windows (ntbackup)**, que maneja la información completa del sistema de archivos, la situación puede cambiar.

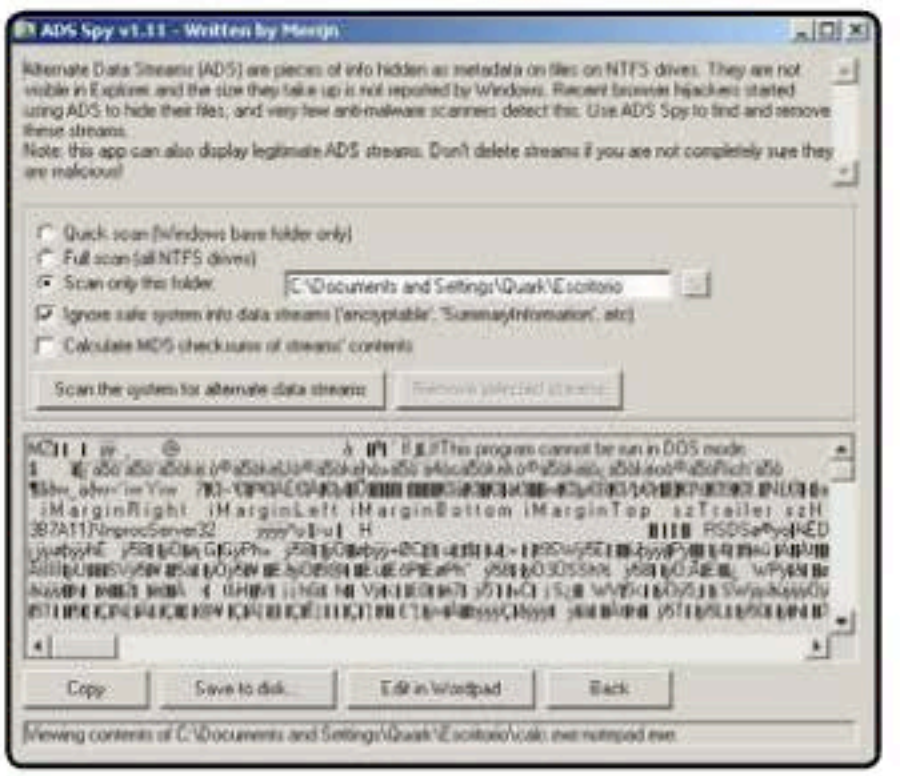


Figura 39. ADS Spy es una herramienta que permite buscar, listar y borrar información contenida en ADS.

Aunque Microsoft no brinda las herramientas directas para visualizar los ADS, podemos utilizar algunos métodos indirectos a través del administrador de tareas, donde es posible observar la información completa de un proceso en caso de que haya sido lanzado haciendo uso de un ADS.

¿MALWARE SOLO EN WINDOWS?

Existe malware que afecta a sistemas Linux y Mac, además de a Windows. Si bien esto puede parecer a primera vista imposible, basta decir que gran parte de las infecciones están vinculadas al comportamiento del usuario y no del sistema.

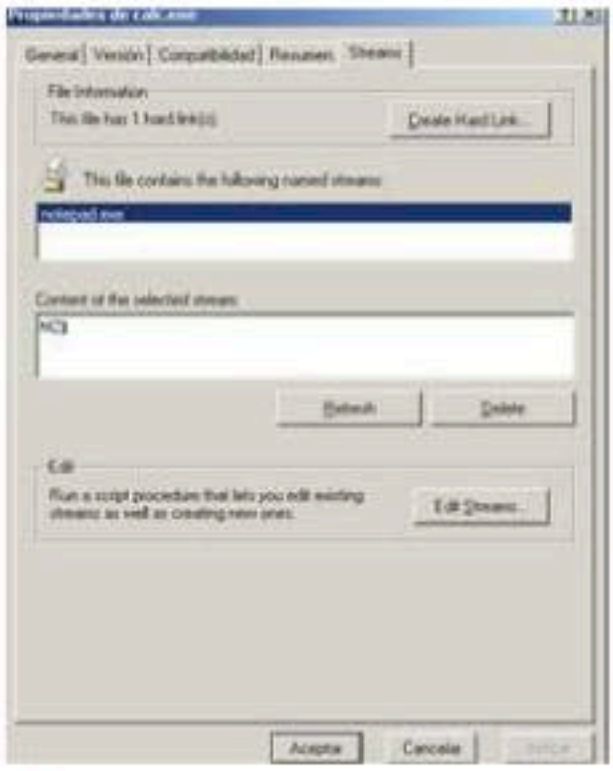


Figura 40. Pestaña de información de ADS dentro de Windows, puede instalarse con algunos pasos sencillos.

Un aspecto que interesa a los atacantes es el de no dejar huellas o minimizarlas. Un atacante con poca experiencia solo pensará en cumplir con el objetivo, en tanto que uno más avanzado considerará los detalles, probablemente, los que marquen la diferencia entre ser descubierto o no, y entre un experto y un principiante. Las huellas pueden quedar en todos los lugares que son utilizados, desde la red hasta el sistema operativo, y los mecanismos de auditoría serán los responsables de hacer que toda la información pueda ser recopilada y analizada.

Figura 41. WbStego es una herramienta con licencia GPL para ocultar información en archivos BMP, de texto, HTML y PDF.

Los rastros a través de Internet estarán signados por el camino de los paquetes a través de la red, desde el atacante hasta el objetivo. En general, el equipo desde el que se lanzan los ataques no es el mismo que aquel en donde se originan, para evitar que se lo rastree fácilmente. Cada dispositivo de red recibirá paquetes del atacante y los transmitirá hacia destino, y si almacenan logs, las acciones pueden ser rastreadas. En cuanto al enlace a Internet, un atacante no utilizará una conexión propia.

RESUMEN

En este capítulo analizamos las distintas etapas de un Penetration test. En la primera identificamos las fuentes públicas desde las cuales obtenemos la información. Describimos la fase de escaneo y sus pasos. Presentamos la etapa del ataque y control sobre un objetivo. Finalizamos, con la fase de mantenimiento del acceso.

Capítulo 4

Técnicas de ataque

En este capítulo veremos las técnicas que sentaron las bases de ataques sofisticados.

RedUSERS.com

Técnicas básicas

Las técnicas básicas que veremos en este capítulo pueden componerse para realizar ataques sumamente complejos, por lo que no deben ser desestimadas por su simpleza. Estas son, tal como se las conoce en la jerga: poisoning, sniffing, spoofing, hijacking, bruteforcing y denial of service.

ENVENENAMIENTO DE LA RED: POISONING

La técnica de poisoning o envenenamiento consiste en redireccionar el tráfico de usuarios a sitios controlados por un atacante. Suele implementarse a partir de la manipulación de los protocolos ARP y DNS.

El **ARP poisoning**, también conocido como **ARP spoofing**, consiste en generar una serie de peticiones y respuestas ARP modificadas con el objetivo de asociar la dirección MAC del atacante con la dirección IP del gateway, para que todo el tráfico de ese segmento pase siempre por el atacante para que este pueda analizarlo y redirigirlo.

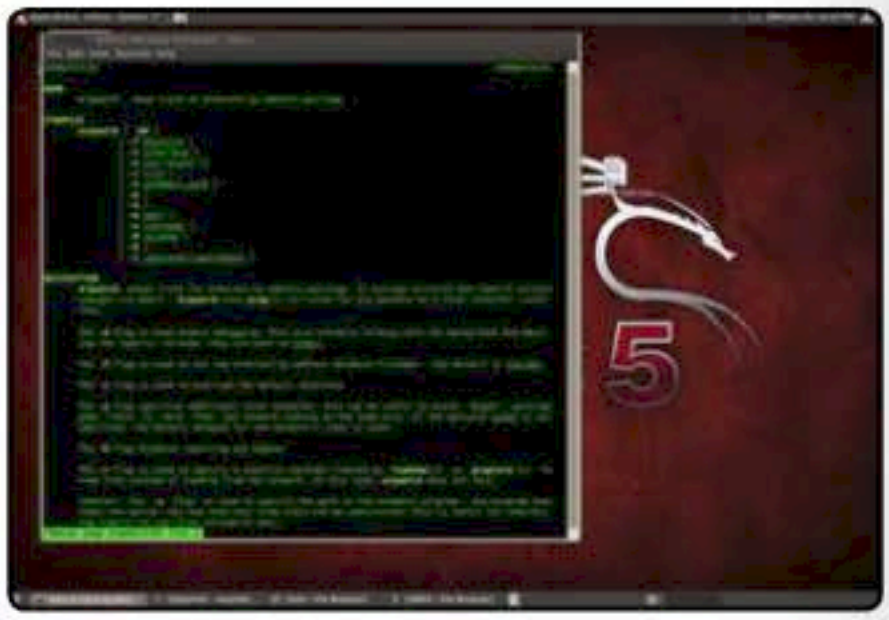


Figura 1. **Manual de** arpwatch, **utilizado para detectar cambios en la asociación entre direcciones MAC e IP.**

El **DNS cache poisoning** consiste en hacer de manera maliciosa que un servidor DNS reciba datos de una fuente no autorizada, de manera tal de contaminar su tabla caché. Así, si un atacante puede controlar dicha tabla, podrá modificar la relación entre la dirección IP y la URL asociada, haciendo que cuando un cliente lícito quiera acceder a un sitio web, en realidad acceda a otro controlado por el atacante.

ANÁLISIS DE PROTOCOLOS: SNIFFING

Un **sniffer** o analizador de protocolos es una aplicación utilizada para **monitorear** y **analizar** el tráfico en la red. Permite capturar datos y visualizarlos cuando son transmitidos en

CAPTURA DE TRÁFICO

Para capturar el tráfico, 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.

texto plano. Por lo tanto, cualquier protocolo que envíe los datos sin cifrar es susceptible de ser analizado por un sniffer. Dentro de estos protocolos tenemos ejemplos como **HTTP**, **SMTP**, **POP3**, **IMAP**, **Telnet**, **FTP**, etcétera.

Figura 2. Winpcap **es la herramienta que los sniffers utilizan para acceder a la capa de enlace en Windows.**

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 el que reenvía los paquetes al destino que corresponde únicamente.

De todas formas, aplicando **ARP poisoning**, esta limitación puede sortearse.

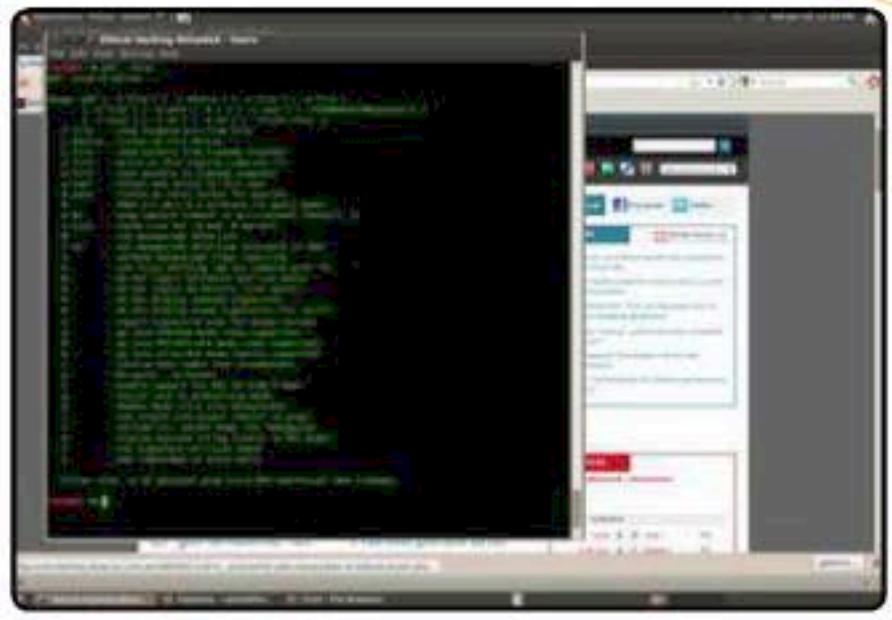


Figura 3. Ayuda de P0f (http://lcamtuf.coredump.cx/p0f3)**, herramienta que utiliza la captura de tráfico pasiva para detectar el SO.**

Podemos diferenciar las técnicas de **sniffing pasivas** y **sniffing activas**. En la primera, también conocida como **eavesdropping**, el sniffer solo se limita a escuchar el tráfico que circula por determinado segmento o contexto sin interactuar. Para que esta técnica sea efectiva desde la óptica de un ataque, suele implementarse en segmentos de red de alto tráfico. En cambio, los sniffers activos, además de capturar tráfico, también pueden enviar paquetes especialmente creados. Esto es muy útil si nos encontramos en una red segmentada mediante switches, ya que, de esta forma, podemos lanzar un ataque de ARP poisoning y así saltear la limitación impuesta por estos.

TRÁFICO EXCESIVO

Es importante tener en cuenta que si se genera tráfico en exceso en la red, existen mayores posibilidades de que el administrador identifique que algo extraño está sucediendo en esta y entonces, ser detectados.

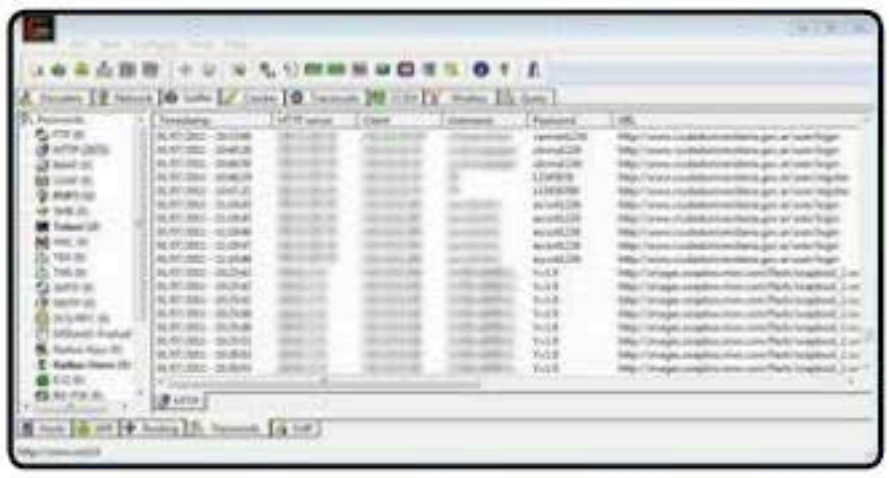


Figura 4. Caín, **en la pestaña de contraseñas se pueden ver algunas de ellas.**

Existen otros analizadores de protocolos generales que también son ampliamente utilizados y no debemos desconocer. Quizás el más famoso sea **Wireshark** (ex **Ethereal**). Es utilizado sobre todo para analizar y detectar problemas en redes y como herramienta didáctica. Permite ver el tráfico de red, usualmente Ethernet, aunque es compatible con otras, configurando la placa de red en modo promiscuo.

Figura 5. Ejemplo de visualización del tráfico de una red Ethernet utilizando Wireshark.

IMPERSONALIZACIÓN: SPOOFING

El **spoofing** es una técnica utilizada para **suplantar la identidad** de otro elemento, que puede ser un usuario, un proceso u otro. Las más conocidas son **IP spoofing**, **MAC spoofing** y **mail spoofing**.

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 utilizando programas que implementen esta técnica o, incluso, modificando los paquetes a mano.

Es importante tener presente que las respuestas del host que reciba los paquetes irán dirigidas a la IP falsificada. Por ejemplo, si se envía un ping spoofeado, la respuesta será recibida por el host que posee la IP spoofeada.

ROBO DE SESIONES: HIJACKING

El concepto de **hijacking** proviene de la palabra inglesa cuyo significado es **secuestro**. En el ámbito tecnológico, hace referencia a toda técnica 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 el spoofing.

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, las 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. En la misma línea, una versión que ya tiene

unos años pero que se sigue usando es el **clickjacking** o secuestro de los clics del mouse.

La combinación de las técnicas de sniffing, spoofing y hijacking nos permiten lanzar ataques más complejos, como el secuestro de sesiones SSL o **SSL hijacking**. Herramientas como **evilgrade** permiten lanzar ataques de mayor nivel de sofisticación combinando o haciendo uso de algunas de las técnicas antes vistas.

Figura 6. Pantalla de inicio de Evilgrade junto con el comando de ayuda desplegado en pantalla.

FUERZA BRUTA

Los ataques de fuerza bruta buscan vulnerar mecanismos de autenticación basados en usuario y contraseña. Para esto, se prueban todas las combinaciones posibles del espacio de claves de un sistema. Por ejemplo, si nuestra aplicación solo permite claves de 8 caracteres y letras minúsculas, el espacio estará determinado por 27^8 claves en total, es decir, 282.429.536.481 claves. Cuanto mayor sea la potencia de cálculo, más rápido podremos encontrar la contraseña.

Figura 7. El comando hashdump de Meterpreter permite obtener un volcado de la SAM del equipo comprometido.

A medida que el espacio de claves y su longitud crece, la capacidad de cálculo se vuelve insuficiente para recorrer el espacio de claves en tiempos prácticos. Por esta razón, muchas veces, en vez de fuerza bruta pura, se utilizan diccionarios con claves organizadas mediante algún criterio, como palabras en español o en inglés o claves por defecto de dispositivos.

Estos ataques pueden ser remotos, cuando se lanzan a un servicio específico desde una ubicación externa; por ejemplo, un ataque a un servicio

SPOOFING FÍSICO

Una analogía del spoofing podría hacerse cuando una persona manda una carta. Si en el remitente en vez de colocar su dirección indica la de su vecino, cuando el receptor la reciba y la conteste, la respuesta llegará al vecino, y no a quien realmente la envió.

FTP, Telnet, SSH, etc. Herramientas como **Hydra**, **Medusa** o **Brutus** permiten implementarlos.

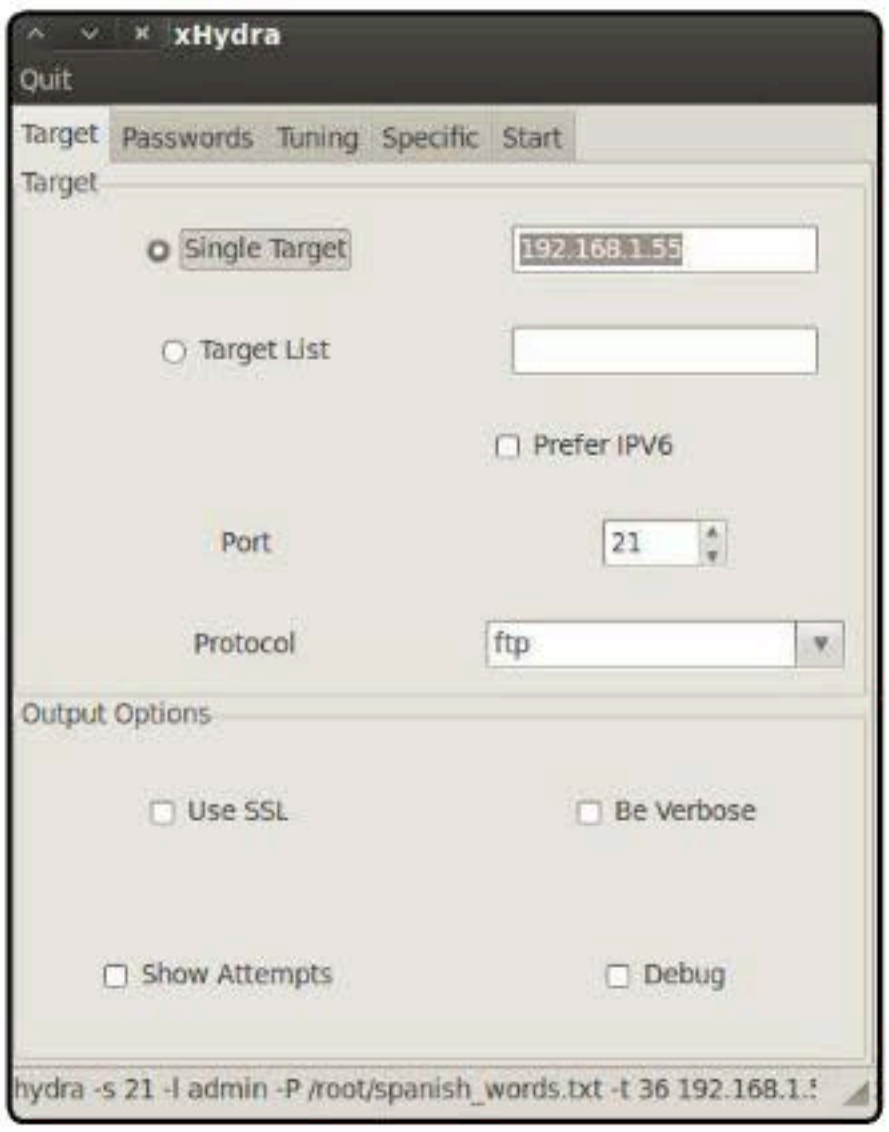


Figura 8. Configuración de xHydra para un servidor FTP con el usuario admin y el diccionario spanish_wordlist.

También pueden aplicarse estos ataques a mecanismos de autenticación locales, como es el caso del logon a los sistemas operativos. En Linux la información de usuarios está almacenada en el archivo **/etc/passwd**, mientras que los hashes de las contraseñas se encuentran en **/etc/shadow**. De esta forma, si un usuario malintencionado puede acceder al archivo **/etc/shadow**, mediante fuerza bruta intentará obtener las contraseñas. Para archivos locales, la herramienta **John The Ripper** es una de las más utilizadas.

Figura 9. John The Ripper en acción. A partir de un ataque de diccionario, se obtuvo la clave del usuario root.

En Windows, la información de cuentas está en **/Windows/System32/config/SAM**. Si un usuario puede acceder, podrá atacar por fuerza bruta, aunque aquí el archivo solo es accesible por el proceso **LSASS** (Local Security Authority SubSystem) y para tener acceso el atacante debería bootear desde un Live CD y así saltear las protecciones de acceso del sistema. Otra opción es utilizar alguna herramienta que realice un volcado de la porción de memoria del archivo **SAM** como **pwdump**.

CONTRASEÑAS Y HASHES

Es importante recordar que ningún sistema operativo almacena contraseñas en texto plano, sino que previamente les aplica una función de hash y luego almacena el resultado asociado a cada una en una ubicación predefinida.

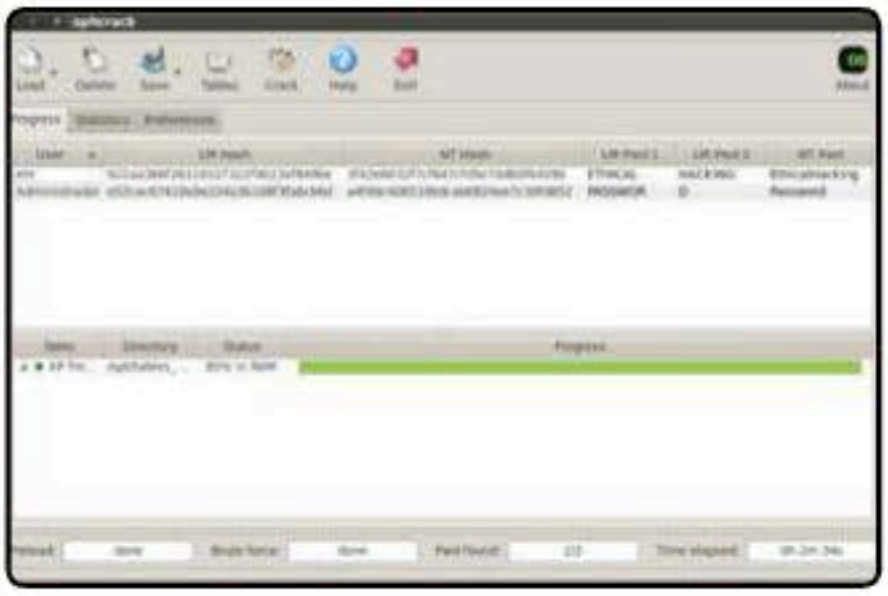


Figura 10. **A partir de la información de hashdump, obtenemos las credenciales del equipo comprometido.**

Hoy en día disponemos de una gran cantidad de herramientas que permiten lanzar ataques de fuerza bruta pura, diccionario e incluso mediante tablas precalculadas (también conocidas como **rainbow tables**).

DENEGACIÓN DE SERVICIO

Los ataques de **denegación de servicio** (DoS) tienen por objetivo saturar los recursos de un equipo o sistema de forma tal de degradar su capacidad de respuesta o, en el mejor de los casos, lograr que deje de responder. Estos recursos pueden ser memoria, capacidad de procesamiento de la CPU, conexiones de red, disco duro, etcétera.

La primera técnica es **IP flooding**, cuyo objetivo es saturar el servicio de red de un equipo o dispositivo determinado mediante el envío de paquetes IP. Puede utilizarse para bajar el rendimiento de la red o saturar los recursos de una víctima para después llevar a cabo un ataque de **session hijacking**. Una forma de potenciar los resultados es utilizar la dirección de broadcast (**broadcast IP flooding**) enviando paquetes a dicha dirección. Existen dos ataques básicos que implementan esta técnica: **smurf** y **fraggle**. Smurf utiliza los 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 llegar a saturar el equipo víctima. El ataque tipo fraggle es similar a smurf, pero utiliza UDP. El resultado es que los hosts que tengan activo el servicio **echo** reenviarán el paquete a la víctima y los que no, mandarán un ICMP de error.

También existen vulnerabilidades de denegación de servicio que permiten que un servicio

VULNERABILIDADES Y DENEGACIÓN DE SERVICIOS

En muchos casos los ataques de denegación de servicio se deben a vulnerabilidades en aplicaciones, como la asociada MS12-020 de Microsoft. Explotando una vulnerabilidad en el Terminal Service, es posible hacer que el equipo deje de responder.

puntual deje de responder, aunque el equipo siga respondiendo y funcionando. Por ejemplo, la vulnerabilidad de **Slow Denial of Service**, presente en varias versiones de los servidores web Apache.

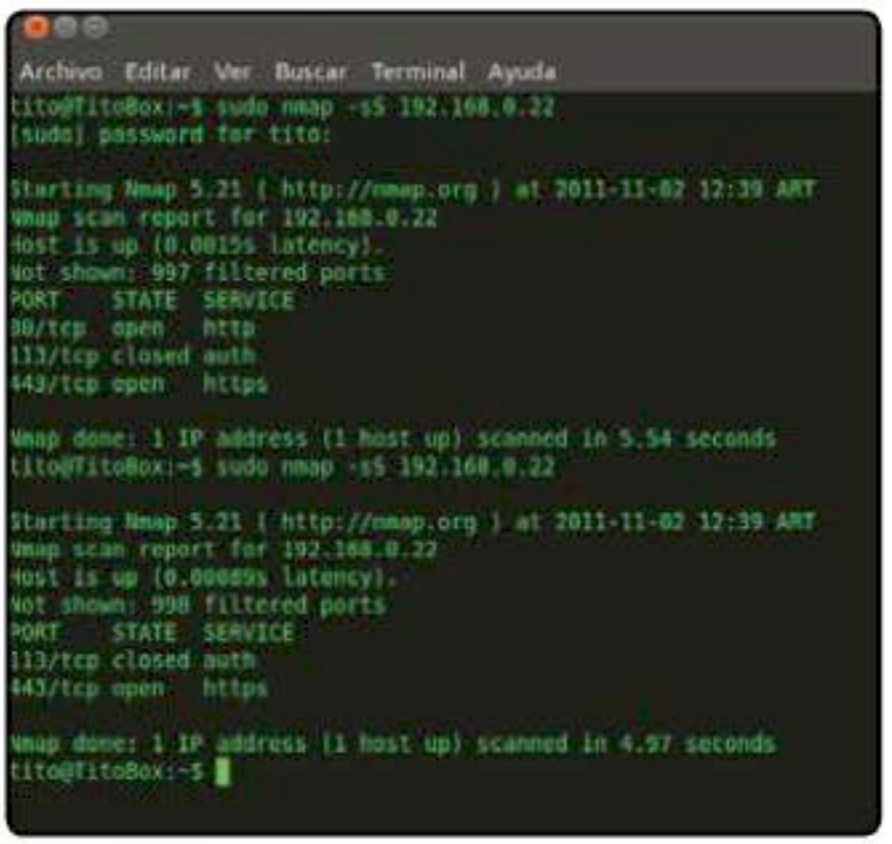


Figura 11. Resultado de NMAP antes y después de ejecutar slowloris a un Apache.

Si ampliamos el concepto de DoS y, en vez de ser un equipo el que lanza el ataque, contamos con un conjunto de ellos, normalmente una **botnet**, estamos en presencia de un ataque de **denegación de servicio distribuida** o **DDoS** (Distributed Denial of Service).

Ataques a **aplicaciones web**

Algunos ejemplos de las aplicaciones web más utilizadas pueden ser los webmails, los foros de discusión, las redes sociales y también, los blogs.

La forma de encarar su seguridad es bastante distinta de la manera de plantear la seguridad convencional. La sencillez de las técnicas y metodologías de intrusión las hace mucho más críticas porque no hace falta gran conocimiento técnico para llevarlas a cabo. Cualquier persona que sepa usar muy bien una computadora y con cierta curiosidad puede hacerlo.

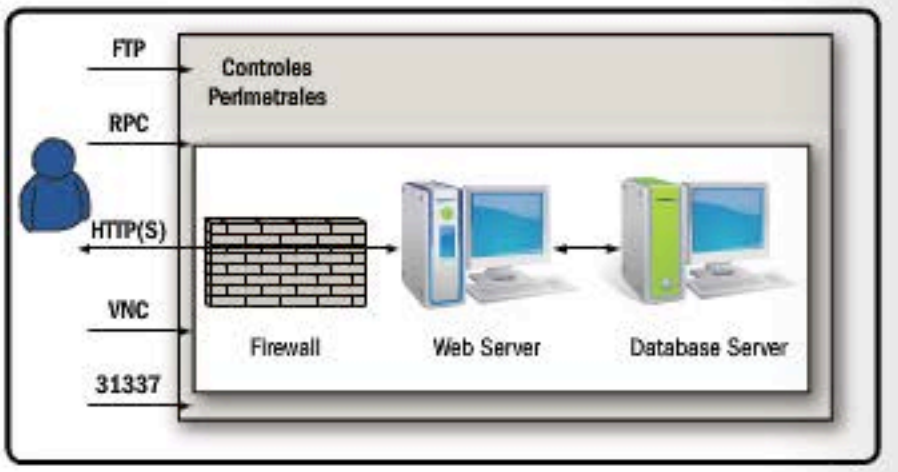


Figura 12. Un intruso intenta acceder a la red a través del puerto 31337 hacia el servidor de bases de datos.

TIM BERNERS-LEE

Una de las personalidades más destacadas en la historia de Internet es, sin dudas, Sir Timothy John Berners-Lee (nacido en 1955 en Londres), por ser considerado el padre de la Web, tal como la conocemos en la actualidad.

Para la mayoría de los firewalls e IDS está permitido interpretar el tráfico del puerto 80, por lo que este debe analizarse internamente con el fin de evitar el envío de código malicioso y también el compromiso de las aplicaciones web de los servidores.

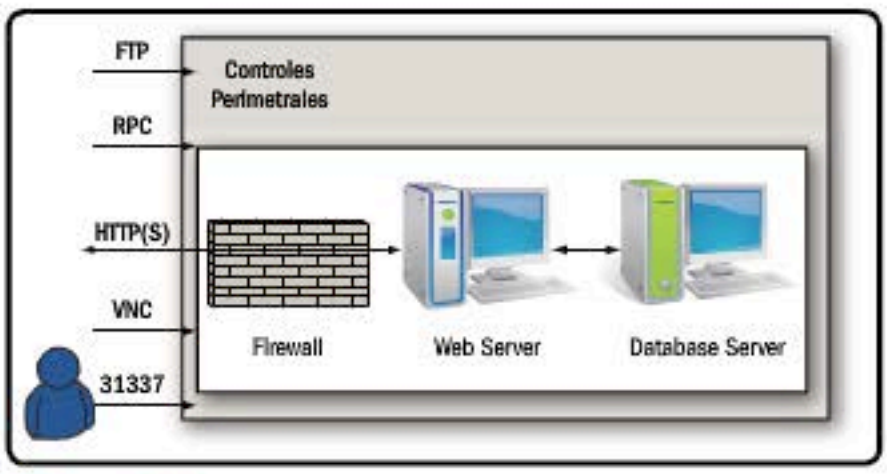


Figura 13. Un intruso accede a la red a través del puerto 80 sin ser filtrado por el firewall.

Los servidores y las aplicaciones web ofrecen diferentes mecanismos de autenticación; el más común de ellos quizá sea el método HTTP, que puede dividirse en:

- **Autenticación básica**: el cliente envía al servidor el usuario y la contraseña en texto plano.
- **Autenticación digest**: calcula la función hash de la contraseña y utiliza un modelo de desafío-respuesta para concluir la autenticación, sin enviar la contraseña en plano en ningún momento.

Figura 14. Defacement realizado al sitio de la policía de una ciudad del estado de Texas, EE.UU., en el año 2012.

También se permite la autenticación basada en NTLM, certificados, tokens y biométricas, entre otras opciones.

Los ataques a las aplicaciones web son de lo más variados. A continuación, detallaremos algunos comunes y sus contramedidas. Los casos de **XSS** e inyección de código también son válidos como amenazas, pero lo veremos más adelante en este mismo capítulo.

Una técnica se basa en la **inyección de comandos** o **command injection** enviando código a un sistema introduciéndolo a través de una aplicación.

WEBGOAT

WebGoat es una aplicación web J2EE deliberadamente vulnerable, creada por la comunidad OWASP, y diseñada para aprender lecciones de seguridad en aplicaciones web. En cada lección, el usuario debe explotar vulnerabilidades reales en la aplicación.

Suele incluir llamadas al sistema vía system calls (syscalls), el uso de programas externos mediante comandos shell (por ejemplo, a partir de CGI) además de llamadas a las bases de datos.

El **poisoning,** por su parte, permite que un atacante inyecte contenido malicioso y obtenga información no autorizada. Para reescribir los datos de una sesión, mostrar los datos de determinada **cookie** (que se usan para mantener el estado de una sesión) o especificar otros identificadores de sesión, se suele usar una aplicación proxy. Incluso hay plugins de los navegadores que permiten manipular las cookies almacenadas.

Figura 15. Extensión de Firefox Add & Edit Cookies**, que interpreta y modifica las cookies almacenadas en el navegador.**

Otra técnica es la llamada **Parameter/Form Tampering**, también conocida como **manipulación de parámetros y formularios**, se aprovecha del hecho de que muchos programadores confían en el uso de campos ocultos y fijos para efectuar operaciones críticas como única medida de seguridad. Si un atacante modifica el valor de un campo oculto, puede cambiar el comportamiento de la aplicación de acuerdo con el nuevo dato incorporado. Estos ataques permiten el robo de servicios, el escalamiento de acceso y el secuestro de sesión. Un ejemplo de **Parameter Tampering** se produce al cambiar el valor de los parámetros dispuestos en los campos de un formulario (con el plugin de Firefox **Tamper Data** es posible realizarlo).

Otro tipo de ataque es **Directory Transversal**, y ocurre cuando un atacante es capaz de navegar directorios y archivos fuera del acceso normal de la aplicación. Expone la estructura del directorio de la aplicación y, en función de la magnitud de la debilidad, la exposición puede abarcar los directorios de los servidores web y los sistemas operativos. El atacante puede utilizar esta técnica para enumerar contenido, acceder a páginas seguras o restringidas (que no se podrían acceder de otra manera),

FIREFOX ADD-ONS

Muchas herramientas de seguridad web pueden presentarse como plugins para Firefox. Un recurso muy útil es FireCAT (Firefox Catalog of Auditing exTensions) que reúne distintos plugins para realizar auditoría de sitios web.

obtener información confidencial, localizar código fuente, y más.

La inyección de código, específicamente, se refiere a la explotación causada por el procesamiento de datos no válidos. Puede ser usada por un atacante para introducir código en aplicaciones con el fin de cambiar su comportamiento. Si bien también se aplica a los programas binarios, librerías y sistemas, en este caso solo nos referimos a entornos web.

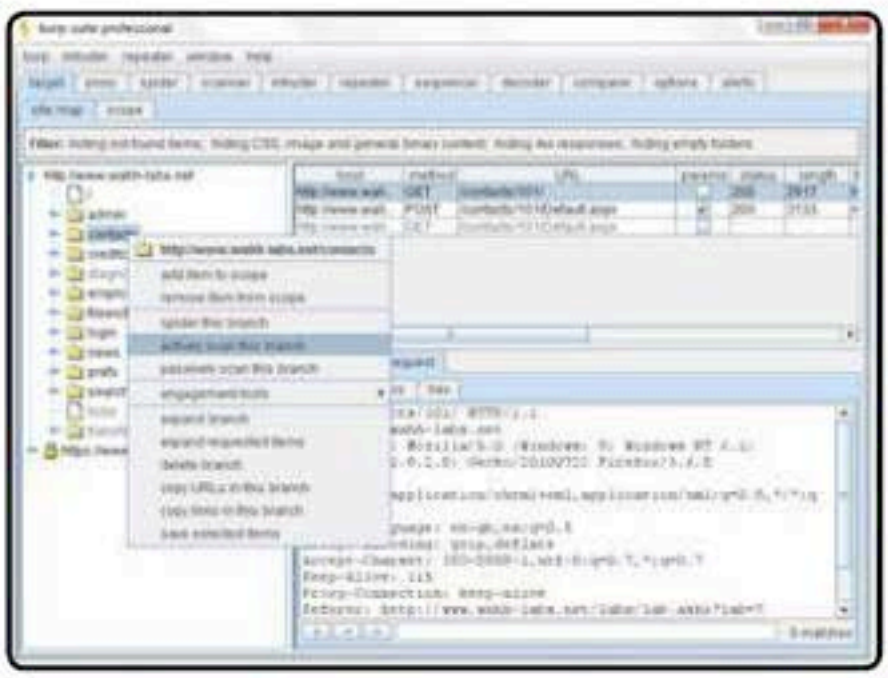


Figura 16. **Consola de** Burp Suite, **una herramienta utilizada para lanzar ataques de inyección de código.**

Muchos optan por utilizar extensiones del navegador, a fin de tener integrada la plataforma de ataque en el mismo navegador. En ese sentido, varios plugins pueden ayudar al atacante.

En HTML hay un etiqueta propia que invoca al objeto script. Esto es, el lenguaje llama a un script (Visual Basic Script, ActiveX, Flash o JavaScript, entre otros) que realiza una función en particular, extendiendo el potencial del lenguaje. Los ataques de **HTML Scripting** tienen por objetivo inyectar código de modo que sea retornado como parte del output de una aplicación, modificando su comportamiento según lo solicitado.

Figura 17. **Extensión de Firefox** UrlParams, **que permite visualizar y modificar los parámetros de una petición http.**

Existe una serie de aplicaciones que utilizan HTML pero que no necesariamente están

ligadas a los entornos web, como la recepción y el envío de correos electrónicos con texto enriquecido, archivos de ayuda, **GUI** (Graphic User Interface) etcétera. De ahí la importancia de HTML Scripting y su relación con la seguridad, ya que muchas más aplicaciones emplean HTML como base. Por otro lado, cada motor de **renderización** de HTML agrega funciones extra según el desarrollador (la ejecución de determinados tipos de scripts, la instalación de plugins, applets, etc.). Además, cada navegador tiene su propio motor de renderización.

Estos recursos le brindan al desarrollador la posibilidad de crear aplicaciones con mejores funcionalidades, pero desde el punto de vista de la seguridad, al sumar funcionalidades, se agrega más código y la probabilidad de error se incrementa, lo que se traduce en un aumento de las posibilidades de explotación.

En HTML se utilizan caracteres especiales para distinguir el texto que se muestra, del código y el formato. Estos tags pueden afectar el formato de la página o también introducir código para ejecutarse del lado del cliente (en este caso será necesario que el navegador tenga la capacidad de interpretarlos)

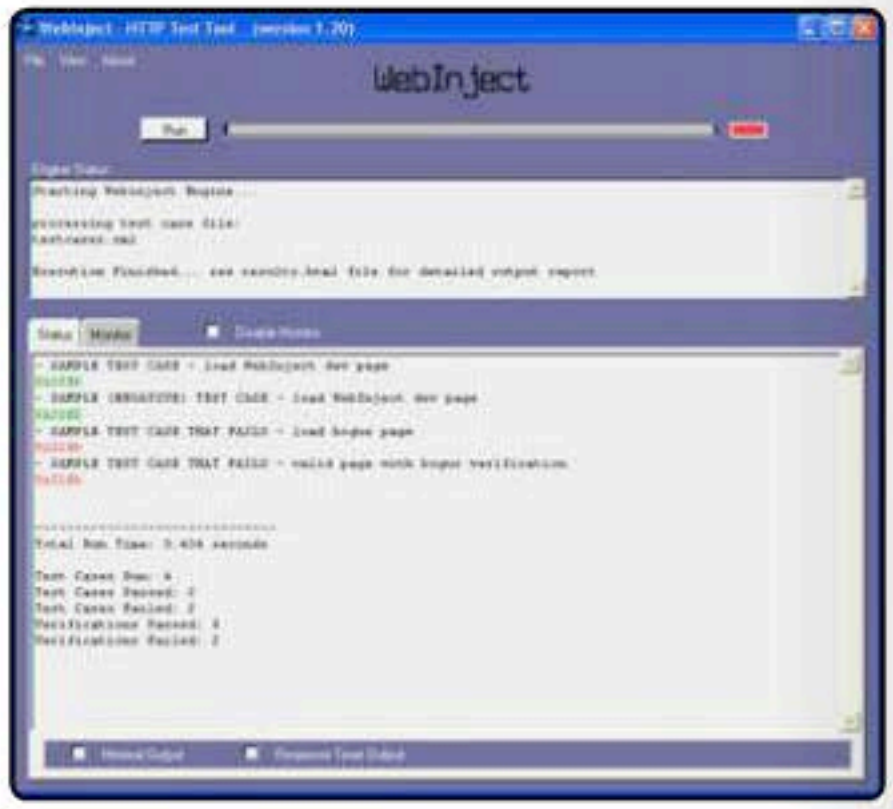


Figura 18. **Consola de** WebInject http Test Tool, **que muestra el estado de las respuestas de los ataques enviados.**

Los tags de scripting más usados para embeber contenido malicioso son **<script>**, **<object>**, **<applet>**, **<embed>** y **<form>**. También puede utilizarse una nomenclatura alternativa de **escritura inline**, como: **javascript:alert('Soy una alerta')**.

El tag **<script>** determina un código de script; que puede estar ubicado en cualquier lugar del encabezado o del cuerpo de un documento y ser definido dentro del tag HTML script o en un archivo externo.

HTML

El lenguaje HTML (HyperText Markup Language) describe la estructura y el contenido de un sitio web en forma de texto utilizando etiquetas para representar objetos (imágenes, videos, etc.), y está basado en SGML (Standard Generalized Markup Language).

Figura 19. **Resultado de un escaneo realizado con** NStalker, **donde se ordenan las vulnerabilidades por nivel de riesgo y los objetos que afecta.**

El **Cross-Site Scripting** o **XSS** es una técnica a partir de la cual se fuerza a un sitio web a ejecutar el código suministrado por un atacante, pero cargándolo en el navegador del usuario. Por esta razón, se dice que es un ataque "del lado del cliente". El código puede ser HTML, JavaScript, VBScript, ActiveX, Java, Flash o cualquier tecnología soportada. El ejecutante logrará que el servidor devuelva un script, sin contar con el nivel de permisos para realizarlo, pero no modifica nada en el servidor, solo inyecta código que luego se ejecuta del lado del cliente. El ataque se lleva a cabo cuando el código del servidor (**server side-code**) toma la entrada ingresada por el usuario y la repite de modo que los datos sean ejecutados como script en el cliente. Las aplicaciones más susceptibles de ser víctimas son: blogs, chats, libros de visita, webmails, formularios de confirmación, y otros.

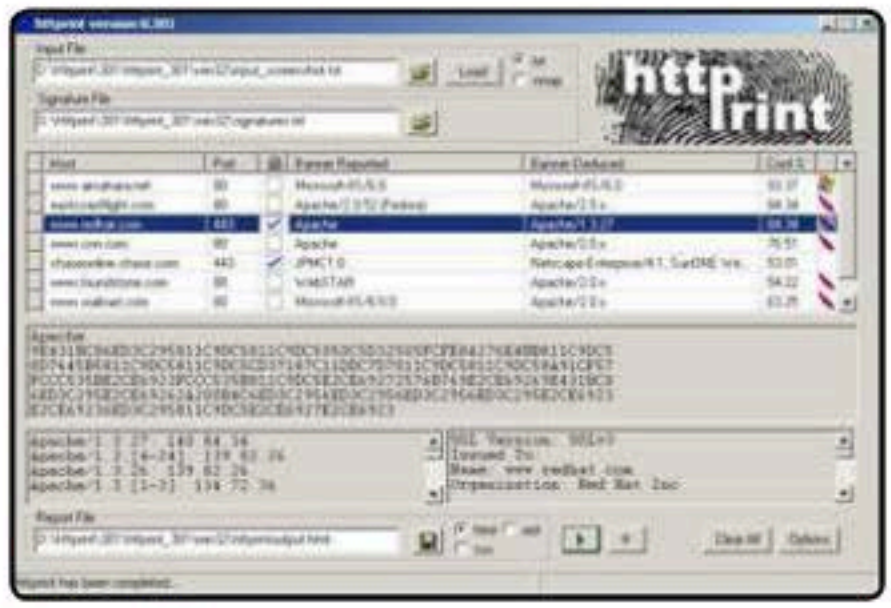


Figura 20. Httprint **identifica de forma remota la aplicación y la versión de un servidor web.**

Según la manera en que se generen pueden categorizarse en: **XSS reflejado** y **XSS persistente**. El primero se produce cuando los datos provistos por un cliente web son usados inmediatamente por el **server-side script** a efectos de generar una página de resultados para mostrarle al usuario. Este es el tipo de XSS encontrado con más frecuencia, y un ejemplo de esto es el que vimos unos párrafos previos. El

MENSAJES DEL PROTOCOLO ARP

Cuando un host quiere comunicarse con una IP, emite un paquete ARP-Request a la dirección de broadcast solicitando la dirección MAC del host. El equipo con la IP pedida responde con un paquete ARP-Reply indicando su MAC.

segundo es similar en cuanto a los efectos, pero se genera de forma distinta, ya que en este caso los datos brindados por el atacante son almacenados en el servidor (bases de datos, sistemas de archivos, etc.).

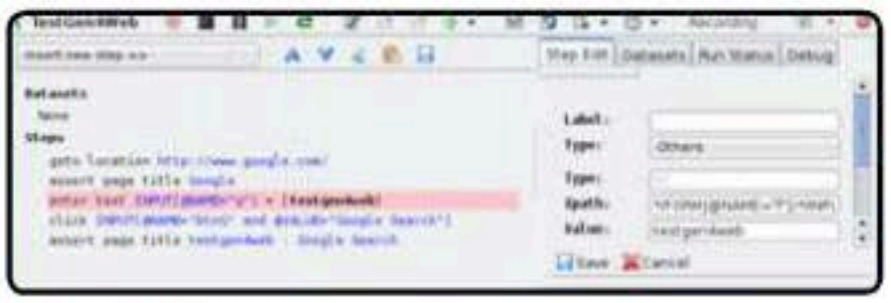


Figura 21. **Extensión de Firefox** TestGen4Web, **que graba las acciones realizadas con el navegador.**

Finalmente, existen los ataques de **SQL Injection**. Conceptualmente, el lenguaje SQL se utiliza para acceder y realizar consultas a la base de datos que interactúa con la aplicación. Un atacante puede utilizar esta técnica contra una aplicación web vulnerable para obtener acceso a su base de datos. La vulnerabilidad se origina en el chequeo incorrecto de las variables de un programa que contiene o genera código SQL. En definitiva, se logra que el motor interprete de manera incorrecta la sentencia enviada y a continuación devuelva un resultado esperado por el atacante.

RESUMEN

En este capítulo analizamos algunas técnicas específicas de ataque por red con las que se pueden construir otros más complejos. Estudiamos algunos ataques utilizados a través de Internet, relacionados con el tipo de tecnología y lenguaje utilizados en la creación de aplicaciones web.

Capítulo 5

Seguridad física

Veremos conceptos sobre los procedimientos de control para protección de amenazas físicas.

RedUSERS.com

Amenazas a la seguridad **física**

Las amenazas son hechos que suelen producir un daño y causar pérdidas de activos, pudiendo ocurrir en cualquier momento. Comúnmnete, se dividen 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 fraudes, vandalismo, sabotajes, espionaje, etcétera) o no intencionales (resultantes de acciones inconscientes).

Biometría

La biometría consiste en el estudio de métodos automáticos para el **reconocimiento de personas** basado en rasgos de conducta o físicos. Etimológicamente, este palabra proviene del griego, en donde **bios** significa vida y **metron** quiere decir medida. En nuestro campo de trabajo, se trata de la aplicación de métodos matemáticos y tecnológicos para identificar o verificar la identidad de los usuarios.

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

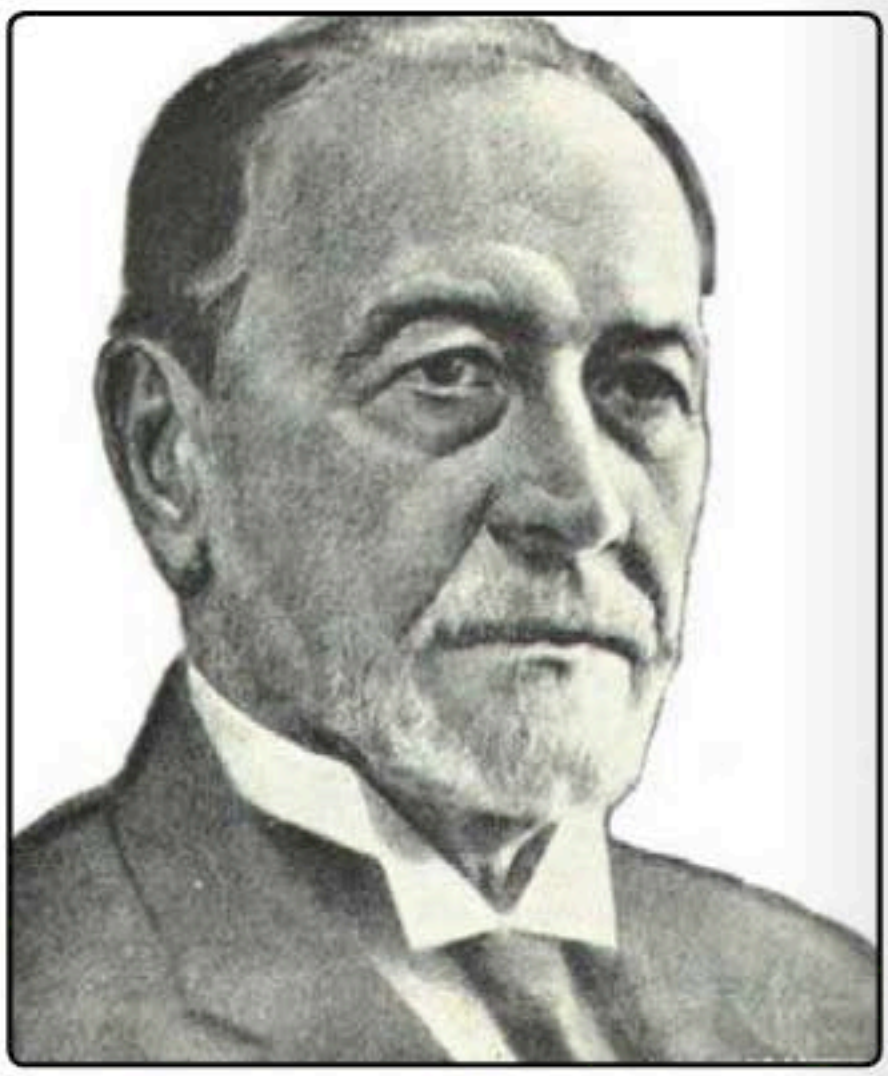


Figura 1. **Juan Vucetich desarrolló y puso en práctica un sistema de identificación de personas por huellas digitales.**

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 de carácter **dinámico** (de comportamiento)

como la firma y el tecleo. La voz, por su parte, se considera una mezcla de características físicas y de comportamiento.

Una huella dactilar, por ejemplo, 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**.

Entre las tecnologías biométricas, existe también el reconocimiento facial, una de las más nuevas y aceptadas porque es una forma común de reconocerse entre personas.

Hay dos enfoques predominantes en este caso: el **geométrico**, que está basado en rasgos y el **fotométrico**, basado en lo visual.

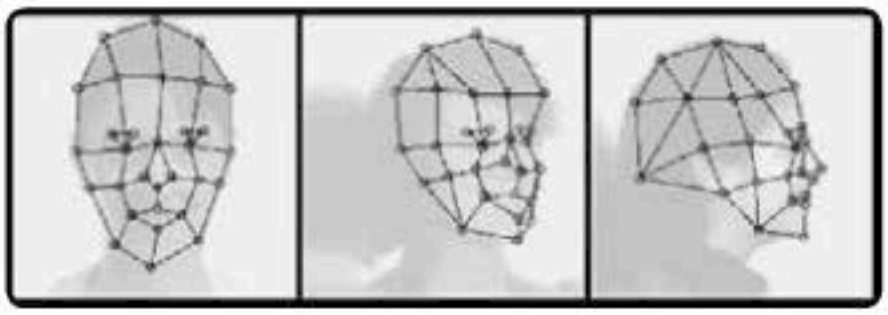


Figura 2. **El reconocimiento de rostro se basa en la correspondencia entre agrupaciones llamadas** grafos elásticos.

El iris y la retina también se utilizan en biometría, para su reconocimiento, primero se realiza la localización y luego la extracción de características, que se comparará con patrones previa aplicación de procesos matemáticos. La ubicación y la disposición de los vasos sanguíneos de la retina, por cierto, es única para cada ser humano, 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 utilizar lentes). Una gran ventaja de este método es que el órgano cadavérico no tiene utilidad para el reconocimiento.

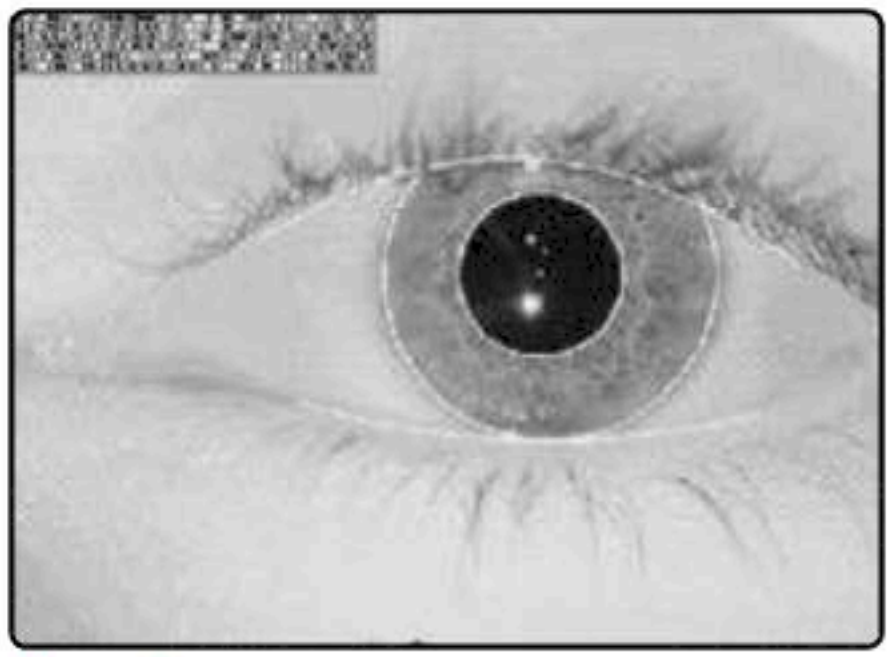


Figura 3. **Los contornos blancos indican los límites del iris y del párpado.**

VENTAJAS Y DESVENTAJAS

La principal ventaja de un sistema biométrico es su dificultad para falsificarlo. Además no puede transferirse ni olvidarse y no requiere esfuerzo en su uso. Sin embargo, su costo es elevado y puede existir rechazo de los usuarios si son invasivos.

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. Funciona mediante la digitalización del habla. Cada palabra se descompone en **segmentos** que tienen tonos dominantes, y se plasman en un espectro para 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.

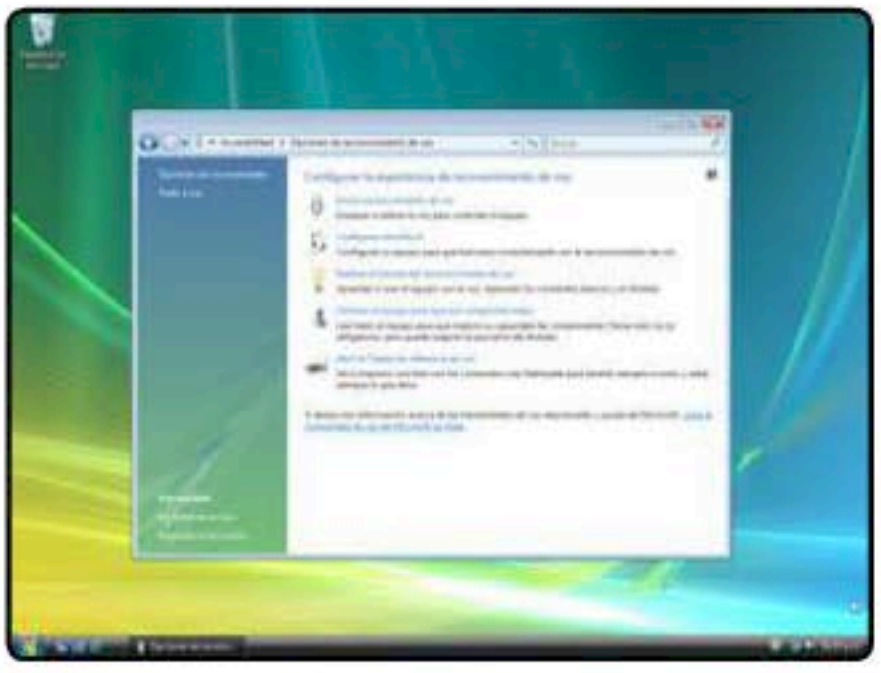


Figura 4. **Vista incluye el reconocimiento de voz, lo que permite ejecutar comandos y aplicaciones mediante el dictado de órdenes.**

Figura 5. **El reconocimiento de firma se utiliza principalmente en bancos e instituciones financieras.**

Protección del datacenter

Sabemos que 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, esta es, sin dudas, la habitación más protegida de un entorno corporativo. Su estructura interior es bastante particular en comparación con otros ambientes. En el

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 y con un sistema antisísmico.

ingreso suelen utilizarse procedimientos donde quede constancia del acceso y de las acciones que realiza cada persona que entra para un futuro análisis.

Figura 6. **Los sistemas de acondicionamiento de aire deben ser calculados en función del volumen de la habitación, en metros cúbicos.**

La ubicación del datacenter dentro de las instalaciones de la empresa determina, en parte, su seguridad.

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

Esto se traduce en la necesidad de contar con sistemas alternativos de provisión, como **grupos electrógenos** o **generadores**.

Figura 7. **El** matafuegos **es la medida básica de seguridad, y el gas más utilizado en datacenters es el** Halotron.

Cuando hablamos de dispositivos complementarios nos referimos a aquellos sistemas de **alimentación ininterrumpida** o **UPS** (Uninterruptible Power Supply), que pueden proteger contra cortes de luz, bajas de tensión, variación de frecuencia, ruido de línea,

PELIGRO, INTRUSOS

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

picos de tensión y caídas transitorias de electricidad, entre otros problemas. Una **UPS** almacena energía en baterías especiales para interiores y además, se usa para proveer electricidad por tiempos no muy prolongados.

Figura 8. **Los generadores eléctricos funcionan con combustible diesel o similar.**

En el caso específico de un datacenter, como estuvimos viendo, es necesario tomar aún mayores recaudos. Por eso se suele utilizar un **piso técnico**, el cual se encuentra conformado por **placas** intercambiables, que son fabricadas a partir de planchas de acero, que, en general, están pintadas con pintura **epoxi**. Estas placas brindan rigidez estructural y aislación acústica, además de ser **ignífugas**.

Figura 9. **El piso técnico permite pasar cables de electricidad y datos por debajo de él.**

En cuanto a los techos, 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 la necesidad de romperlos.

Finalmente, las **paredes, por lo general,** también suelen ser de materiales ignífugos con tolerancia de, al menos, una hora a la exposición del fuego y lo suficientemente resistentes como para minimizar la posibilidad de cualquier clase de penetraciones.

MEDIDAS CONTRA INCENDIOS

Un tema importante en la protección de datacenters es la detección y supresión de incendios. Un incendio implica la extensión de fuego que afecta a las estructuras y a los seres vivos y puede causar la muerte por inhalación de humo y quemaduras.

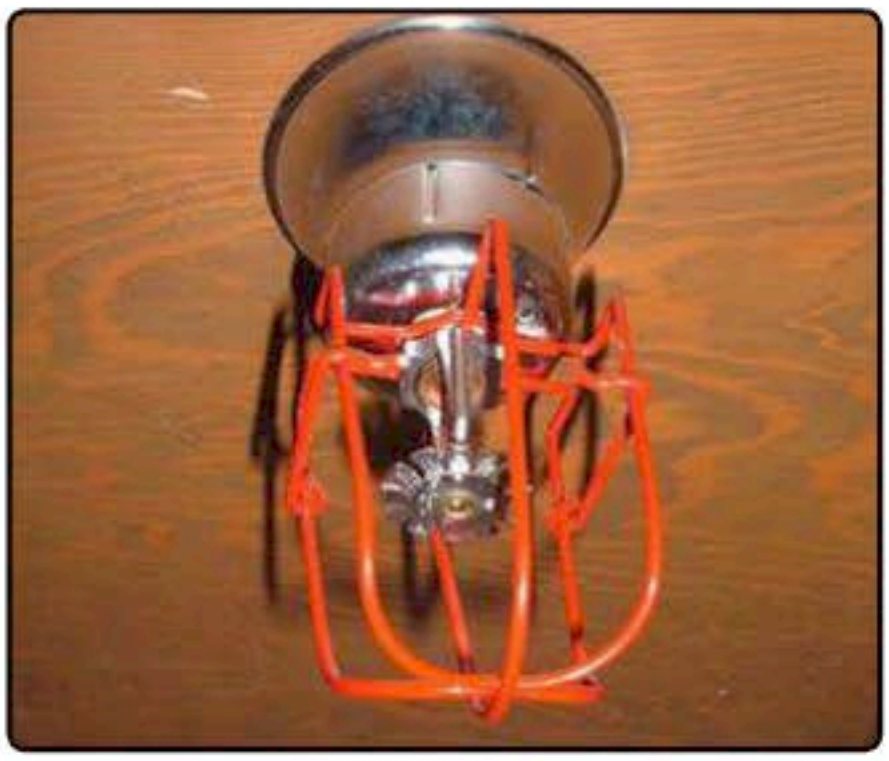


Figura 10. Un sprinkler es un dispositivo para extinción de incendios que libera agua sobre la zona afectada.

Figura 11. Las cerraduras electrónicas son indispensables en los accesos donde hay que registrar y autorizar.

Acceso a las instalaciones

Un correcto control en los accesos a las instalaciones de una empresa determina en gran medida la **protección de los activos**.

Por esta razón es que debe tenerse en cuenta especialmente la seguridad de la organización desde el perímetro externo hasta las vías de ingreso a los edificios, las oficinas y, fundamentalmente, el datacenter.

Primeramente, 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 suelen dividirse por su principio físico de actuación. Si bien su mayor área de desarrollo y aplicación es la seguridad

CERRADURAS ELÉCTRICAS

Una medida que puede romper con el lockpicking tradicional son las cerraduras electrónicas, que son dispositivos que operan igual que una cerradura, pero con la ayuda de un circuito eléctrico, y en general con una botonera para insertar un código.

nacional en instalaciones militares, gubernamentales, prisiones, fronteras, aeropuertos y demás, también se destaca su uso en las industrias, las sedes de empresas, las residencias de alto nivel, etcétera.

Figura 12. **Las puertas pueden incluir cerraduras activadas por tarjeta magnética para aumentar la seguridad.**

En cuanto a las puertas, se deberán utilizar las de alta seguridad para prevenir impactos e ingresos por 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, razón por la cual también son bastante más pesadas.

Figura 13. **Las bóvedas de seguridad de bancos poseen puertas de acceso con el mayor nivel de segurida.**

Para atravesar accesos físicos basados en puertas con cerraduras, se aplican técnicas de **lockpicking** (del inglés **lock**, que significa

CLASES DE COMPUERTAS

Las compuertas de acceso a instalaciones se clasifican en: entradas residenciales, comerciales, entornos industriales y accesos restringidos. Las diferencias estriban en las aperturas diarias, el ancho de los vehículos y la seguridad asociada.

cerradura, y **pick**, ganzúa), que se basan en el uso de herramientas especiales que no incluyen la llave original.

La teoría del lockpicking habla de explotar los defectos mecánicos, lo cual requiere conocer la teoría acerca del funcionamiento de los distintos sistemas utilizados.

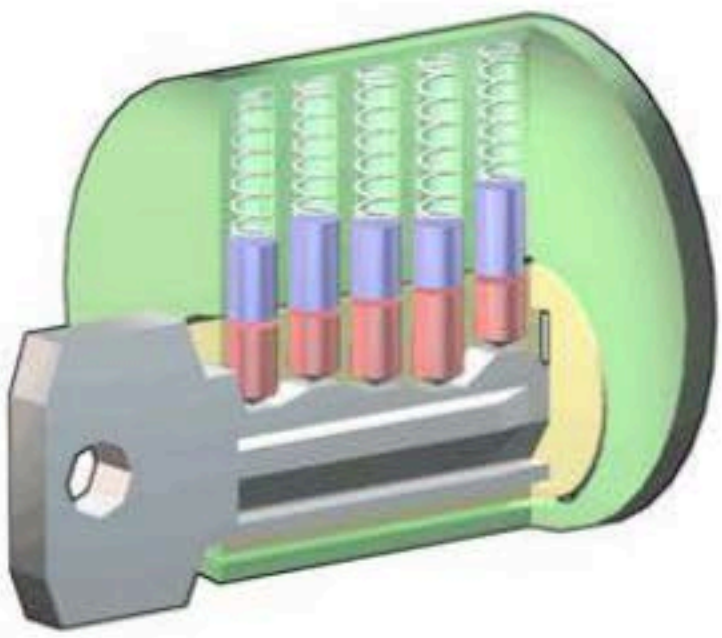


Figura 14. **En sistemas tradicionales de cerraduras primero se intenta el uso de tensión para poder abrirlas.**

Los sistemas más modernos requieren técnicas más refinadas y sobre todo mucha 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 en este casos 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 15. **Los juegos de** ganzúas **son la herramienta indispensable para el** lockpicking.

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 cerraduras tradicionales por su flexibilidad, aunque son bastante más costosas porque requieren mayor mantenimiento.

SELECCIÓN DEL LUGAR

En el momento de elegir la ubicación para una sede corporativa, fuera de las ciudades, la seguridad física incluye la contaminación, las construcciones que hay en la zona, los vecindarios lindantes, la población del lugar y las características de los alrededores.

Monitoreo y detección

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.

Figura 16. **Los sistemas de alarma poseen un teclado numérico que permite activarlos y desactivarlos cuando es necesario.**

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

Figura 17. **Los sensores de movimiento encienden una luz durante el tiempo que detectan la presencia de una persona.**

CONTROL VEHICULAR

Para controlar el ingreso y el egreso de vehículos, el personal de vigilancia debe asentar en una planilla los datos de estos y de los ocupantes, así como también información adicional, para que puedan identificarlos en caso de necesitarlo.

Los **detectores** pueden utilizar diferentes tecnologías dependiendo de 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 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.

Los sistemas de monitoreo, por su parte, 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.

Figura 18. Las cámaras de vigilancia permiten un control visual de todo aquello que ocurre dentro de un ambiente.

Figura 19. Los guardias de seguridad realizan tareas de reconocimiento y de protección.

EL ORIGEN DEL VIGILANTE

La palabra vigilante proviene de **vigil**, los primeros centinelas del emperador Augusto en la antigua Roma. Luego se convirtieron en cuerpo elite para seguridad del César y sus funciones eran mantener el orden público en la ciudad y actuar en incendios.

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. La principal desventaja del personal de guardia es que puede ser sobornado por un tercero para lograr el acceso, lo cual debe tenerse en cuenta en la elección de las medidas de control.

Figura 20. Los sistemas de seguridad en algunos parques industriales pueden llegar a tener fuertes medidas de defensa perimetral.

RESUMEN

En este capítulo vimos aspectos referidos a los componentes físicos de la seguridad. Describimos la biometría y los elementos del cuerpo humano que son estudiados. También presentamos la seguridad a nivel del datacenter y las amenazas que de esta se desprenden, principalmente en los accesos y en la protección del entorno.

Capítulo 6

Ingeniería social

En este capítulo veremos las formas de amenazas que se aprovechan de la vulnerabilidad humana.

RedUSERS.com

Un ataque **sin tecnología**

En el campo de la seguridad de la información, la **ingeniería social** es la práctica para obtener datos confidenciales a través de la **manipulación psicológica** de los usuarios legítimos. La técnica se puede utilizar para conseguir información, acceso o privilegios en sistemas, que permitan realizar algún acto que perjudique o exponga a una persona o empresa a riesgos y abusos. El principio en el que se sustenta la ingeniería social es aquel que afirma que en cualquier sistema los usuarios representan el eslabón débil de la cadena.

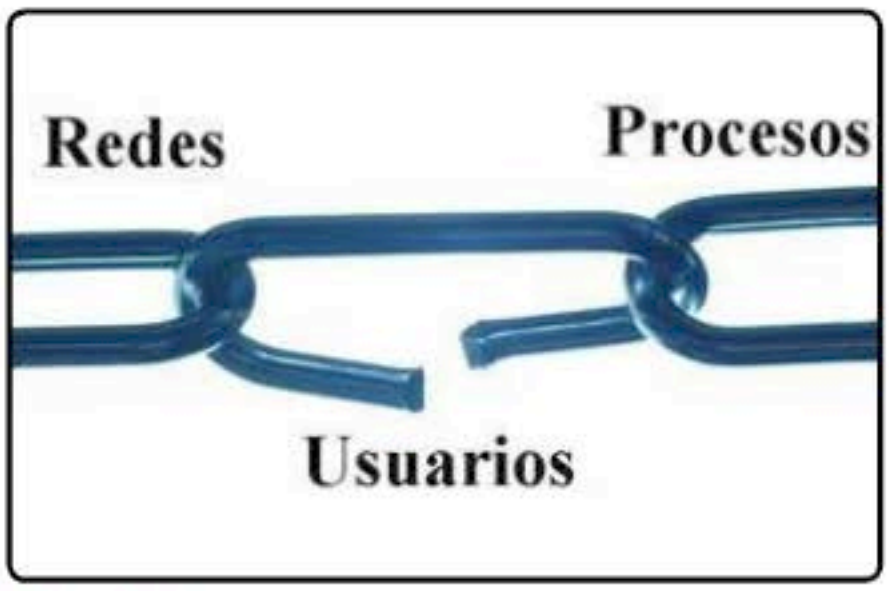


Figura 1. Siempre los usuarios son el eslabón que se rompe con mayor facilidad.

A través de Internet suelen enviarse solicitudes para renovar credenciales de acceso a sitios, e-mails falsos que piden respuestas e, incluso, las famosas cadenas, que llevan a revelar información sensible o a violar políticas de seguridad.

De esta manera, se aprovechan algunas tendencias naturales de las personas en vez de tener que encontrar agujeros de seguridad en los sistemas. Otro ejemplo muy difundido es el uso de **archivos adjuntos** en e-mails, que una vez que se ejecutan diseminan un **código de tipo malicioso**.

Figura 2. En los cubículos de los empleados de oficinas, se encuentra información personal además de datos de la empresa.

EL TELÉFONO ROTO

En la práctica se utiliza como medio el teléfono para engañar a la gente simulando, por ejemplo, ser un empleado de un banco o de una empresa, un compañero de trabajo, un técnico o un cliente y, así, obtener información.

La psicología **humana**

La psicología es la ciencia que estudia la conducta de los individuos, sus procesos mentales, y las influencias que se producen en su entorno físico y social.

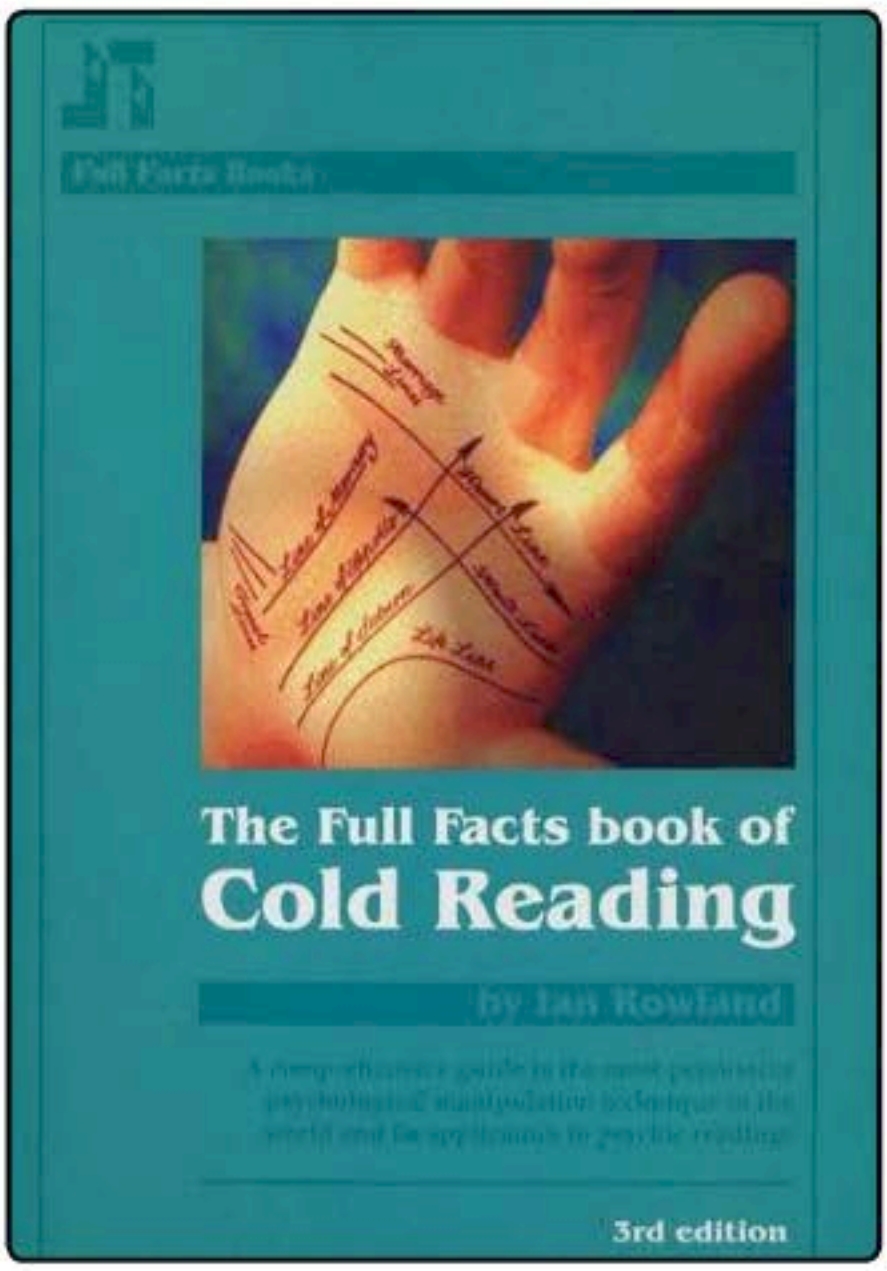


Figura 3. **Un excelente manual sobre lectura en frío es** The Full Facts Guide To Cold Reading, **de Ian Rowland.**

En la seguridad de la información, los aspectos relacionados con la psicología humana son fundamentales, ya que en ellos se basa la manera en que procesan su información personal, manejan sus datos y se comportan en sus distintos entornos.

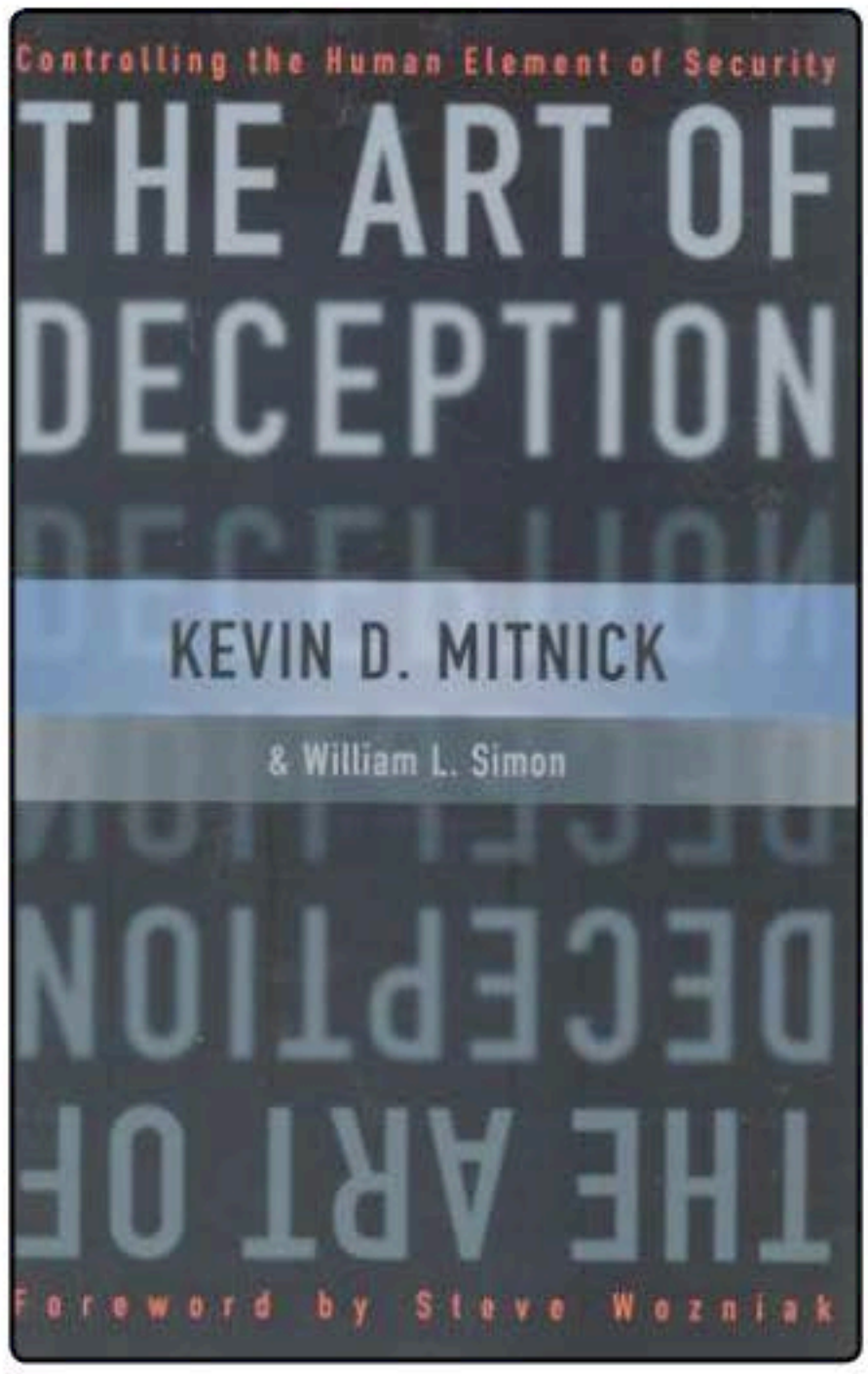


Figura 4. The Art of Deception **es, junto a** The Art of Intrusion, **un libro clásico del especialista Kevin Mitnick.**

Existen comportamientos vulnerables en los que se basa la ingeniería social, como que las personas responden a la autoridad, confían en otras personas, les gusta sentirse halagadas y no les agrada negarse a ayudar.

Algo que un atacante también aprovecha, sin duda, es la generación de sentimientos

variados, como la curiosidad, la avaricia, el sexo, la compasión o el miedo para conseguir su objetivo, que será una acción específica por parte del usuario.

Figura 5. **Una máquina destructora de papel es un accesorio común para eliminar información sensible en las oficinas.**

Sobre la base de la experiencia y la edad, las personas pueden estar más o menos expuestas al peligro de ser engañadas mediante un ataque de ingeniería social. Por ejemplo, un adolescente que tiene la posibilidad de conocer a una joven no dudará en hacer cualquier cosa para conquistarla. En ese caso, el atacante podría hacerse pasar por una jovencita que no entiende de Internet, y requerir ayuda de un muchacho que pueda resolverle sus problemas.

A medida que las personas crecen van adquiriendo experiencias que dejan enseñanzas sobre la forma de actuar. A veces se genera una verdadera sensación de paranoia en los individuos, que los vuelve extremadamente cuidadosas con la seguridad. Los niños pequeños son mucho más vulnerables a la extracción de información, dado que no son conscientes de la importancia que puede tener cierto dato.

Figura 6. **Un peligro común son los robos ocurridos a la salida de cajeros automáticos.**

Las dos modalidades posibles de contacto son la interacción de persona a persona y la que se lleva a cabo por medios informáticos.

En el primer caso, se requieren habilidades sociales y una buena dinámica interpersonal. Los

EL GRAN INGENIERO SOCIAL

Uno de los ingenieros sociales más famosos de la historia es Kevin Mitnick, quien, sobre la base de su experiencia y conocimientos, escribió los libros The Art of Deception (El arte del engaño) y The Art of Intrusion (El arte de la intrusión).

especialistas en estas técnicas se muestran agradables y confiables, y pueden interpretar distintos personajes con diferentes estados de ánimo según el caso. Al adaptarse a la interrelación con cada persona para hacerla sentir a gusto, las posibilidades de éxito aumentan. Una variante es la comunicación vía telefónica. En este caso, el objetivo principal es manifestar con la voz todos los estados de ánimo que se pretenden y lograr que la víctima haga lo que el atacante necesita con solo escucharlo.

Figura 7. **Las habilidades de comunicación interpersonal hacen que las personas den información sensible a su interlocutor.**

Por último, cuando la interacción se da por medios electrónicos, el atacante requiere menos habilidades, ya que no está sujeto a la espontaneidad y puede planificar mejor. Un buen especialista regresará recurrentemente a sus víctimas hasta cumplir con su objetivo. Las personas más comúnmente alcanzadas por estas técnicas son las que mayor conocimiento poseen en función de su actividad. Por ejemplo, algunas de las profesiones más atacadas son la de recepcionistas, encargados y el personal de limpieza de oficinas y edificios, que conocen los movimientos de las personas, incluso, en los ambientes más concurridos, además de los telefonistas.

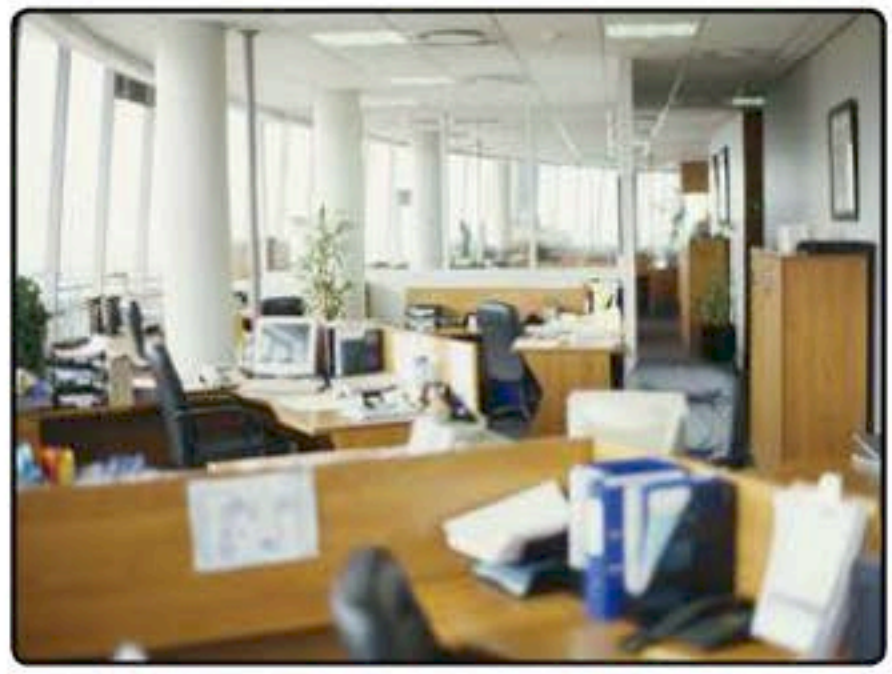


Figura 8. **Una oficina vacía suele ser un espacio ideal para que un atacante encuentre información importante.**

Phishing

El término **phishing**, en informática, denota un uso de la ingeniería social para intentar adquirir información confidencial, por ejemplo, contraseñas, cuentas bancarias, datos de tarjetas, etcétera, de manera fraudulenta. El accionar del **phisher** (los estafadores que utilizan esta técnica) es simple, ya que se hace pasar por una persona o entidad de confianza (por e-mail, SMS, mensajería instantánea o páginas web) imitando el formato, el lenguaje y la imagen de entidades bancarias o financieras. En todos los casos, la comunicación simula ser oficial y suele pedir algún tipo de dato de acceso o información relevante alegando motivos diversos, como verificación de movimientos, cambio de políticas y posible fraude, entre otros.

Figura 9. **Existen muchos recursos audiovisuales para generar conciencia en seguridad.**

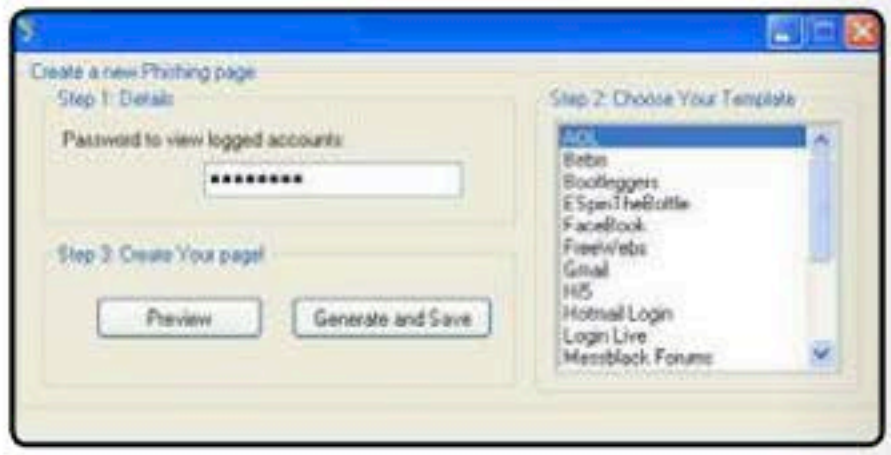


Figura 10. **Los kits de phishing facilitan el trabajo de los atacantes, que pueden desconocer aspectos técnicos.**

El accionar del phisher consiste en envíar mensajes que suelen contener un link a páginas web aparentemente reales de las entidades citadas, pero que, en realidad, conduce a sitios falsos que emulan la página original con el objetivo de **pescar** los datos ingresados por los usuarios. Dado que los clientes pueden ver la página y tienen confianza en la entidad, ingresan sus datos con normalidad, como si se tratara del sitio original, que es fiable.

A partir de ese momento, el phisher puede disponer con total libertad de los datos ajenos, realizar compras por Internet utilizando las tarjetas de crédito, transferencias bancarias no autorizadas, retirar dinero en efectivo de cajeros automáticos, etcétera.

En otros casos, los atacantes monitorean el comportamiento de los usuarios para realizar estudios de mercado y luego venderlos. Los daños causados por el phishing van desde la imposibilidad de acceder al propio **correo electrónico** o **mensajero instantáneo** hasta la pérdida de grandes sumas de dinero.

Figura 11. **En el certificado digital de Internet Explorer podemos comprobar la validez del servidor al que accedemos.**

EL PANORAMA DE LOS PHISHERS

La ganancia de los phishers se da principalmente por la masividad de los ataques y no por la estafa de un usuario en particular. Muchos usuarios son vulnerables a estos ataques por desconocimiento, de modo que para evitarlos se requiere conscientización.

En cuanto al tipo de ataque, existen métodos activos y pasivos. Los activos tienen que ver con la interacción del atacante con las víctimas, en tanto que los pasivos consisten en esperar a que las víctimas caigan en trampas dejadas por los **atacantes**.

Figura 12. XING **es la red social de negocios más importante de Europa.**

En la mayoría de los métodos, además de las ideas originales de los phishers, se utilizan conceptos técnicos de **scripting** o **programación**. Por ejemplo, si recibimos un e-mail con un enlace a un banco y apoyamos el puntero del mouse sobre el link, este puede indicar la URL donde nos llevará. Una técnica consiste en hacer que dicha URL esté mal escrita o utilizar subdominios. También se pueden falsear enlaces utilizando direcciones que contengan el carácter @ (**arroba**). El efecto que se logra con esto es pedir un usuario y una contraseña. Otra posibilidad es usar comandos de **JavaScript** que alteren la barra de direcciones. Esto se consigue colocando una imagen de la URL de la entidad legítima en dicha barra, o bien cerrando la barra original y abriendo una que la emule. Otro problema con las URL está en el manejo de nombres de dominio internacionalizados (**IDN**) en los navegadores. Esto hace que direcciones que resultan idénticas a la vista conduzcan a sitios diferentes, posiblemente, a páginas web con malas intenciones. Esta técnica, conocida como IDN spoofing o **ataque homógrafo**, comenzó a ser muy utilizada en los últimos años.

Figura 13. **Cuadro de información básica presentado por uno de los principales navegadores:** Google Chrome.

ACTA ANTIPHISHING

En marzo de 2005 se promulgó en los Estados Unidos el Acta Antiphishing, una ley federal que establece que aquellos que crearan páginas falsas o enviaran spam para estafar a usuarios podrían recibir multas y penas de encarcelamiento.

Hoy en día, el phishing ha avanzado tanto, que hasta existen **kits de software** que emulan a una gran cantidad de entidades financieras de distintos países, para instalar en un **servidor web** y engañar a usuarios incautos.

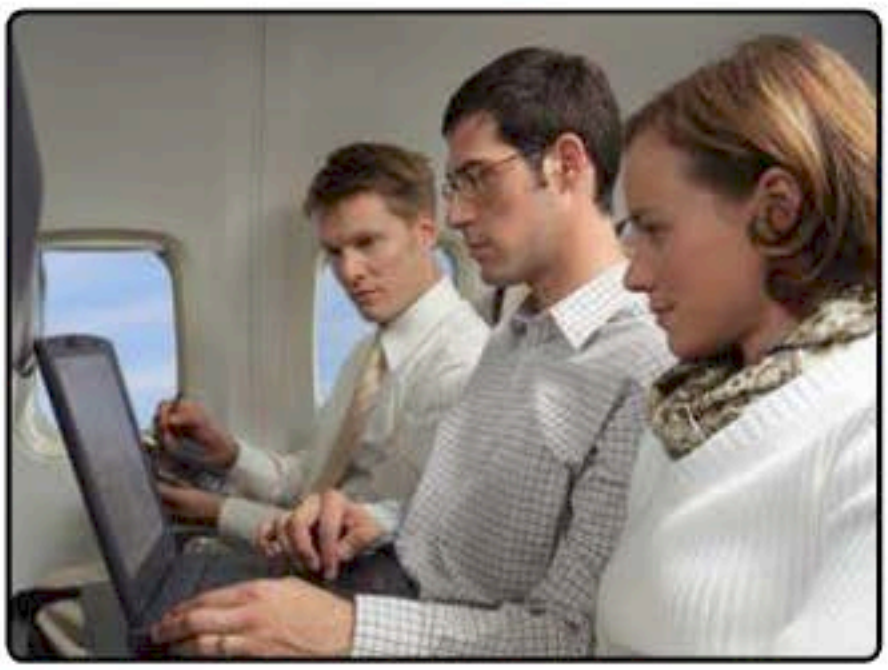


Figura 14. **Alejar la vista del teclado de una persona que está ingresando datos privados es visto como una señal de respeto.**

Redes sociales

Las redes sociales son un **vehículo** ideal para los **atacantes**, ya que presentan un medio de gran potencia que puede tener una alta efectividad, tanto para conectarse con amigos y posibles socios comerciales, como para la averiguación de datos personales. De hecho, un atacante solo necesita llamar la atención de la gente para lograr que haga clic en un link y, así, llevarla a un sitio que el propio atacante controla, para que la víctima se infecte con un código malicioso.

Figura 15. **Sitios como Twitcam combinan una red social con una transmisión por webcam que funciona en vivo.**

Una de las razones por las cuales los sitios de redes sociales han pasado a ser tan peligrosos es el hecho de que puedan incluirse aplicaciones de terceros, que no son fáciles de controlar por las mismas redes, hecho que los convierte en un claro vehículo para la distribución de malware. Lo que hace único al problema

MEMBRESÍAS Y REDES SOCIALES

Muchas personas deciden pagar membresías a redes sociales profesionales y de negocios, para poder de esa manera manejar mejor sus características de privacidad contra su exposición. Esto no está disponible en redes como Facebook o Twitter.

es la solución de compromiso existente entre la **necesidad de estar online**, visible, presente en la red, y al a vez, seguro, protegido, y sin que nadie pueda utilizar maliciosamente dicha información.

Figura 16. **El sitio www.identidadrobada.com es un excelente punto de referencia para prevención del robo de Identidad.**

Explotar la ingeniería social

Como hemos mencionado a lo largo de este capítulo, en varias ocasiones resulta más rentable, desde el punto de vista del ataque, aprovecharse del comportamiento de las personas, que explotar vulnerabilidades técnicas asociadas a los sistemas de información. Para eso existen varias herramientas de software que facilitan el proceso mediante el cual un usuario malicioso puede lanzar un ataque de ingeniería social hacia uno o varios individuos.

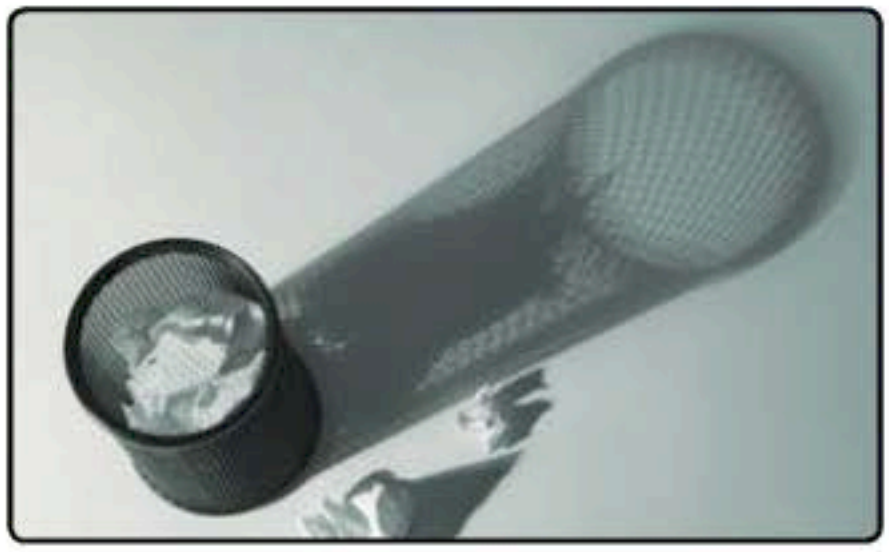


Figura 17. **Un atacante preparado sabe cómo y donde buscar información, por lo que se debe tener cuidado al descartar material.**

A continuación, veremos algunos detalles al respecto y un ejemplo a partir del uso de la herramienta SET.

Los ataques de ingeniería social pueden ser genéricos y estar dirigidos hacia todas las personas que trabajan en una organización; hacia un grupo de ellas, por ejemplo, a quienes trabajan en el área de Recursos Humanos; o bien a una persona específica, como podría ser el gerente general.

FRAMEWORK DE INGENIERÍA SOCIAL

Un recurso invaluable para la ingeniería social es el sitio www.social-engineer.org que cuenta con un framework donde se presenta tanto la base teórica del tema como recursos de utilidad para recopilar información específica y de planificar ataques.

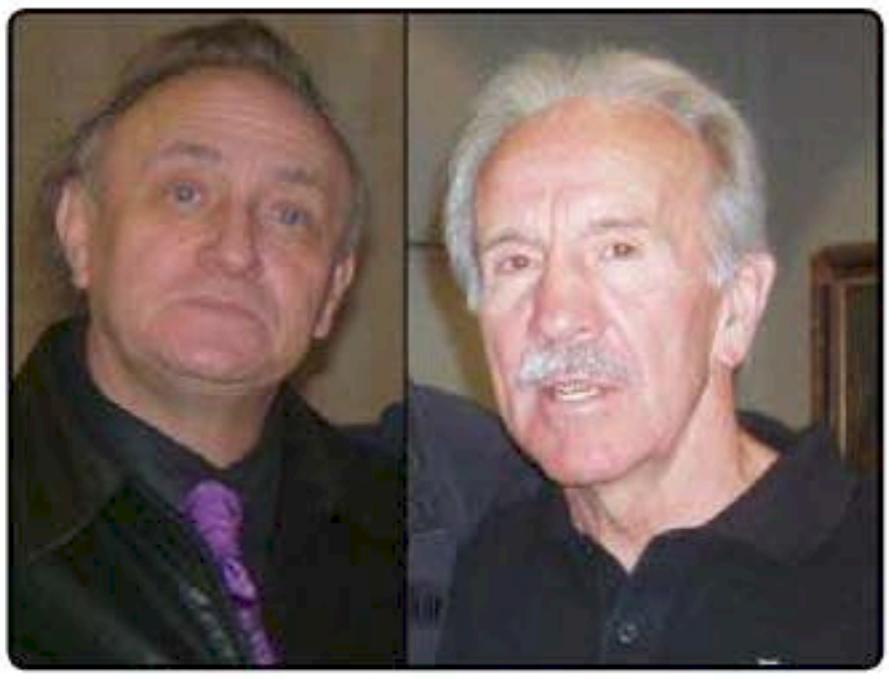


Figura 18. **Richard Bandler y John Grinder fueron los creadores de la PNL, una técnica avanzada que se utiliza en ingeniería social.**

Aunque también es posible encontrar ataques que no están dirigidos, sino que buscan víctimas dispersas en Internet sin ningún criterio específico, estos normalmente no son parte de un test de intrusión, sino que suelen estar relacionados con actividades delictivas. Los ataques de phishing a diversas organizaciones, en especial a entidades bancarias, y la distribución de malware son solo algunos ejemplos.

RESUMEN

En este capítulo analizamos los tipos de ataques que se basan en características y patrones del comportamiento humano. También estudiamos la técnica de phishing como engaño a usuarios, y la función de las redes sociales en la investigación de perfiles.

Capítulo 7

Criptografía

En el este capítulo analizaremos en detalle las bases de la criptografía.

RedUSERS.com

Introducción **e historia**

La mayoría de los avances que se dieron en las distintas etapas de la evolución humana estuvieron ligados a **objetivos militares**, para luego trasladarse a la sociedad civil y comercial. Por ejemplo, al momento de inventarse la rueda, se utilizó en primera instancia en los carros de combate, el hierro para construir armas, la pólvora para generar explosivos, etcétera. El desarrollo y los avances en **criptografía** no escapan a este comportamiento.

Figura 1. **Cifrador del César para el alfabeto castellano. Se realiza un desplazamiento a la izquierda de tres posiciones.**

Durante las guerras, ambos bandos debían enviarle información confidencial a sus tropas o bien a otras ciudades, que, muchas veces, se encontraban a grandes distancias, y para llegar a ellas había que cruzar por territorios controlados por el enemigo. Con esto surgía la necesidad de enviar esa información de forma tal que en el caso de que alguien no deseado la obtuviese, no pudiese comprenderla.

En función del método que se utiliza para ocultar o hacer esa información incomprensible, surge una primera clasificación de los sistemas criptográficos: la **criptografía clásica** y la **criptografía moderna**. En la primera, el secreto del sistema está dado por esconder el mecanismo o **algoritmo** por el cual fue generado el mensaje cifrado. En cambio, en la criptografía moderna, la seguridad del sistema está dada por el secreto de una **llave** que se utilizará para cifrar ese mensaje. Quien posea esa llave podrá cifrar y descifrar esos mensajes.

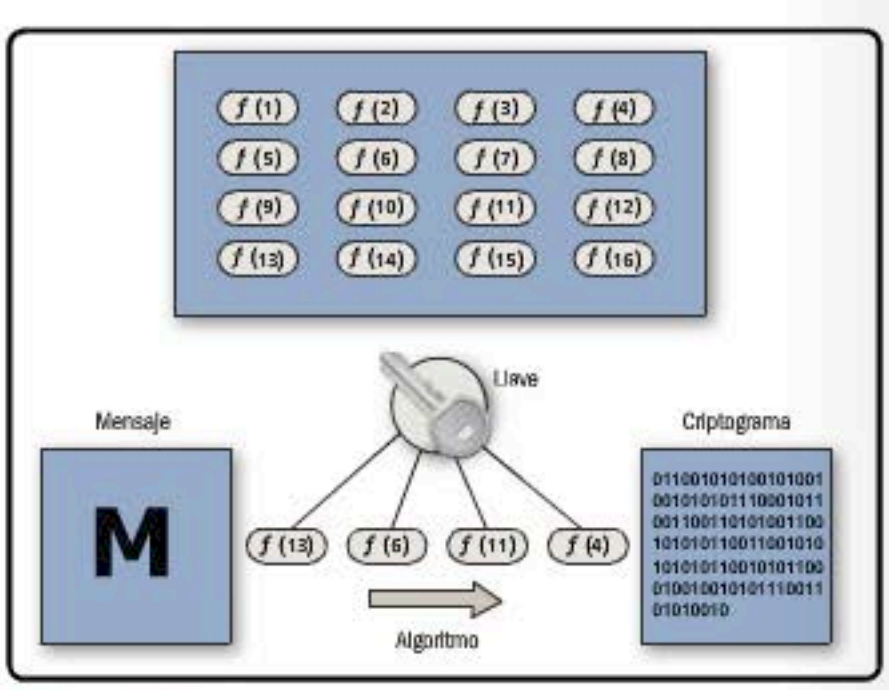


Figura 2. **Esquema de carácter genérico del proceso de cifrado.**

CRIPTOGRAFÍA EN SEGURIDAD

Los principios de la criptografía dan lugar a diferentes tipos de criptosistemas, que a su vez permiten garantizar los tres aspectos básicos de la seguridad: confidencialidad, integridad y autenticidad, y adicionalmente, el no repudio.

En nuestro caso, hablaremos de **algoritmos de cifrado** cuando hagamos referencia a aquel mecanismo por el cual vamos a pasar de un mensaje en texto plano, legible y comprensible por cualquiera, a un mensaje cifrado cuyo contenido es incomprensible si se lo obtiene como tal.

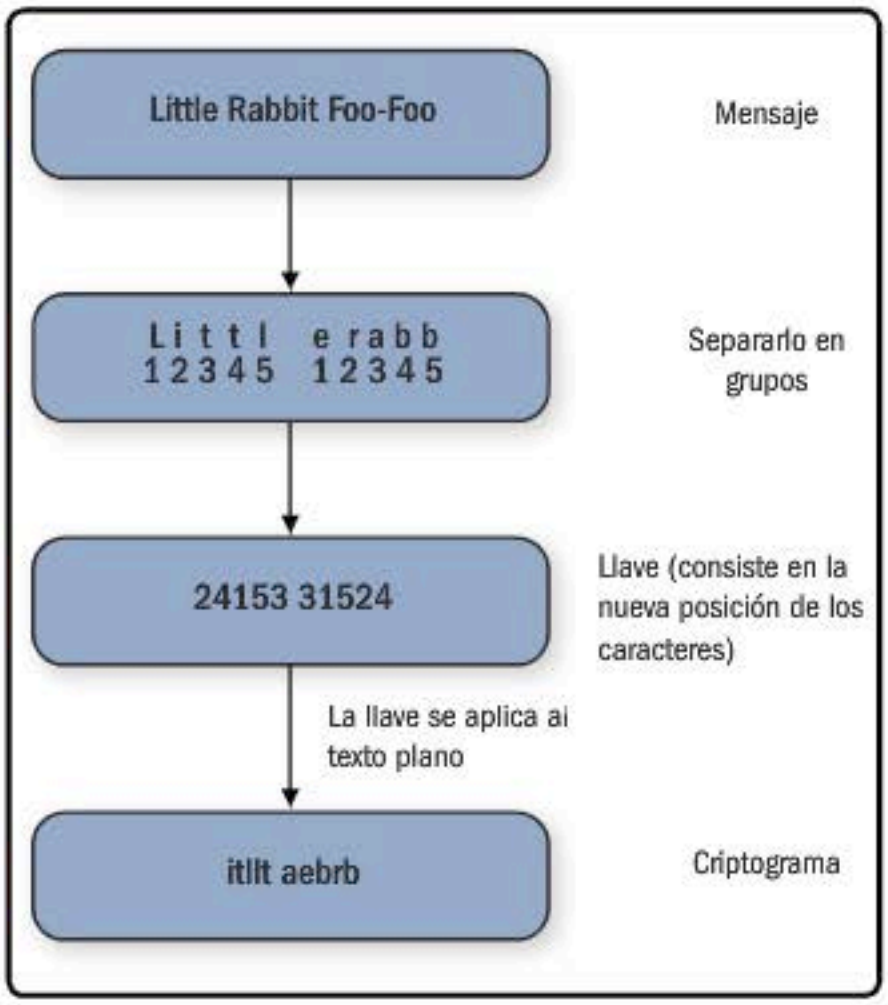


Figura 3. **Ejemplo de técnica de** transposición.

En el caso de la criptografía moderna, vamos a necesitar una o más llaves para poder cifrar y descifrar los mensajes.

Técnicamente se define a la criptografía como la rama inicial de las matemáticas y, en la actualidad, también de la Informática, que hace uso de métodos y técnicas con el objeto principal de cifrar y proteger un mensaje o archivo por medio de un algoritmo, usando una o más claves.

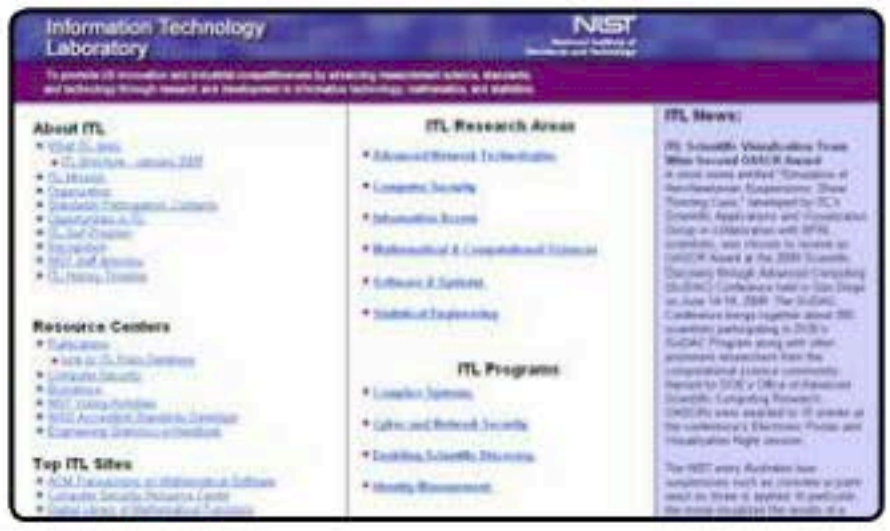


Figura 4. **En el sitio del** Information Technology Laboratory **del NIST accedemos a los estándares publicados por este organismo.**

El criptoanálisis, por su parte, es el estudio de los métodos para obtener el sentido de una información cifrada sin acceso a la información secreta requerida para obtenerlo normalmente. Actualmente, esto se traduce en conseguir la clave secreta del sistema criptográfico, aunque también se utiliza para referirse a cualquier intento de sortear la seguridad de otros tipos de algoritmos y protocolos criptográficos.

EL GURÚ

Bruce Schneier (www.schneier.com) es uno de los criptógrafos actuales de mayor renombre. Es el creador de los algoritmos simétricos Blowfish y Twofish y autor de varios libros de buena aceptación en el ambiente de la seguridad.

Figura 5. Los certificados digitales proveen información para cifrado del usuario que es dueño de este.

Algoritmos **simétricos**

La denominación de **algoritmos simétricos** surge del uso de **una sola clave** para cifrar y descifrar, denominada **clave secreta** o **secreto compartido**. Para enviar un mensaje desde un emisor a un receptor dado, ambos deben compartir la clave.

Aquí surge la debilidad más importante de este tipo de sistemas, ya que trae aparejada la necesidad de un mecanismo de gestión y distribución de claves porque estos algoritmos no los poseen.

Esto hace necesario el uso de mecanismos de distribución externos, por ejemplo, utilizando un mecanismo de **distribución offline** o bien algún algoritmo asimétrico, ya sea por **RSA** o por **Diffie-Hellman**, que analizaremos en detalle en la sección de algoritmos asimétricos. Además no brindan la posibilidad de **autenticar** los mensajes mediante firma digital.

Estos algoritmos se utilizan igualmente porque la velocidad de cifrado es alta comparada con la de los asimétricos. Con claves pequeñas, se obtienen altos niveles de seguridad.

Los tamaños de claves son de 128 o 256 bits, contra 1024 o 2048 bits típicas del cifrado asimétrico. Por otro lado, dado que presentan características no lineales, el único ataque factible es por **fuerza bruta**.

EL CONCURSO DE 1973

Algunos de los requerimientos para el concurso de 1973 fueron: alto nivel de seguridad computacional, fácil de entender y bien especificado, que la seguridad no fuera afectada por su publicación y de uso en diferentes aplicaciones.

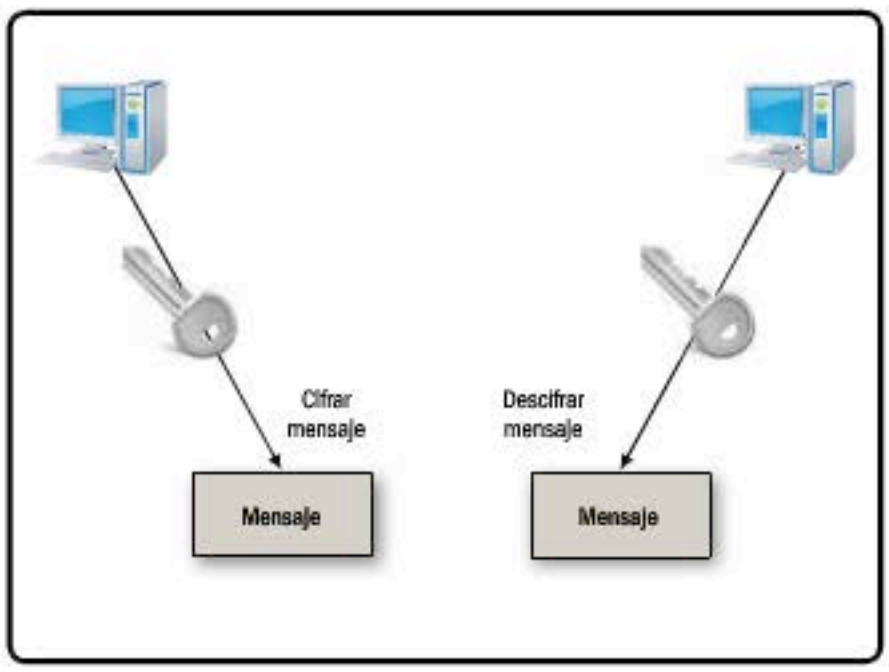


Figura 6. Un algoritmo simétrico utiliza la misma clave en el proceso de cifrado y descifrado.

DES

En 1973, la **NBS** (National Bureaux of Standards) decidió llamar a un concurso público con el objetivo de buscar un algoritmo criptográfico estándar a nivel nacional.

Un año más tarde, la **NBS** tuvo que declarar desierto este primer concurso, publicó las segundas especificaciones y, finalmente, eligió al algoritmo denominado **Lucifer**, pero aplicándole ciertas variaciones.

En 1976, se adoptó **DES** como estándar y se autorizó para que fuera utilizado en comunicaciones no clasificadas del gobierno.

Como podemos ver la tarea de encontrar un algoritmo criptográfico es algo muy complejo, que implicó sucesivos concursos para lograrlo.

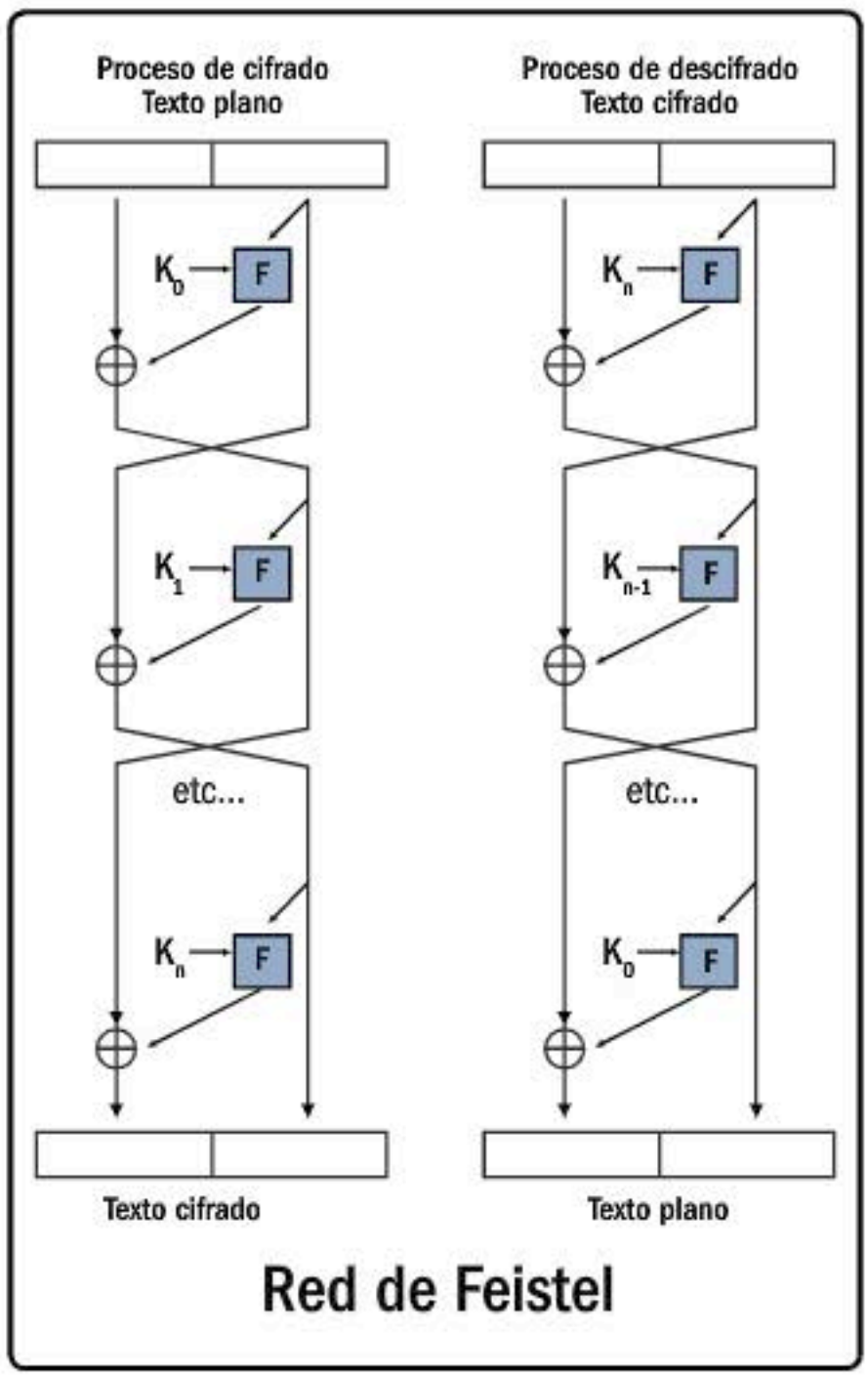


Figura 7. DES se basa en una red de Feistel, donde el esquema de cifrado y descifrado es exactamente el mismo.

EL PODEROSO DR. SCOLNIK

Desde 2005, un reconocido matemático argentino, el Dr. Hugo Scolnik, ha realizado notables avances en la factorización de enteros grandes, que de continuar avanzando podría echar por tierra la seguridad de RSA.

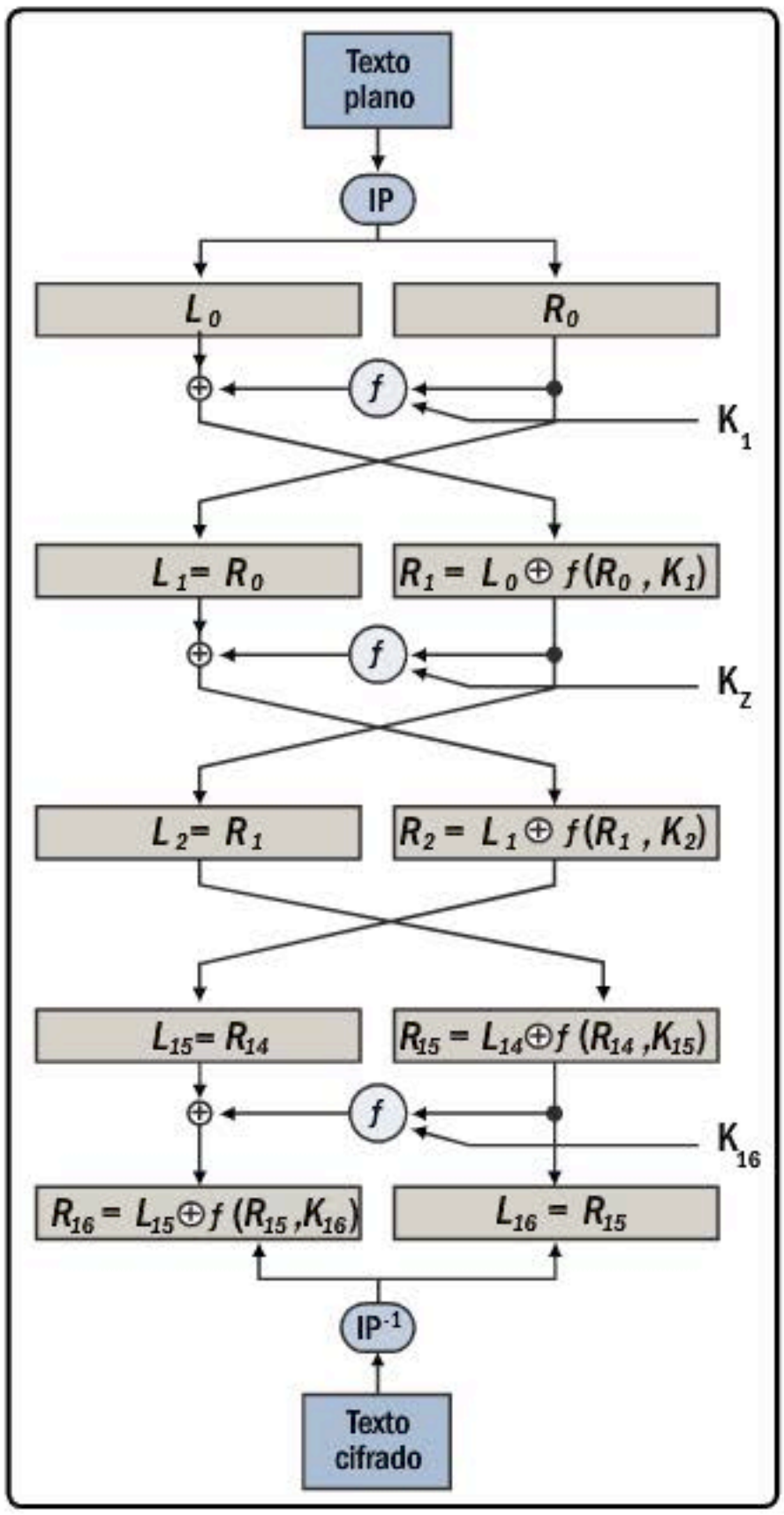


Figura 8. **Proceso general de** cifrado/descifrado **en** DES. **Etapa de permutación, 16 vueltas y etapa de permutación inversa.**

3DES

Debido a las características propias de DES, podemos aumentar el tamaño efectivo de la clave (y por ende el espacio de claves) si ciframos varias veces con claves distintas. De esta forma, aplicando tres veces el algoritmo DES, y dependiendo si utilizamos dos o tres claves, podemos duplicar o triplicar el tamaño efectivo de la clave.

Si bien se tiende a suponer que aplicando dos veces la función DES se duplicará el tamaño de la clave, pero esto no es así. Porque si duplicamos el tamaño de la clave, en este caso solo aumentaremos en 1 bit su longitud efectiva. Por otro lado, el proceso de cifrado con solo dos claves es susceptible de sufrir ataques del tipo **man-in-the-middle**. Por esta razón, se aplica la función DES tres veces.

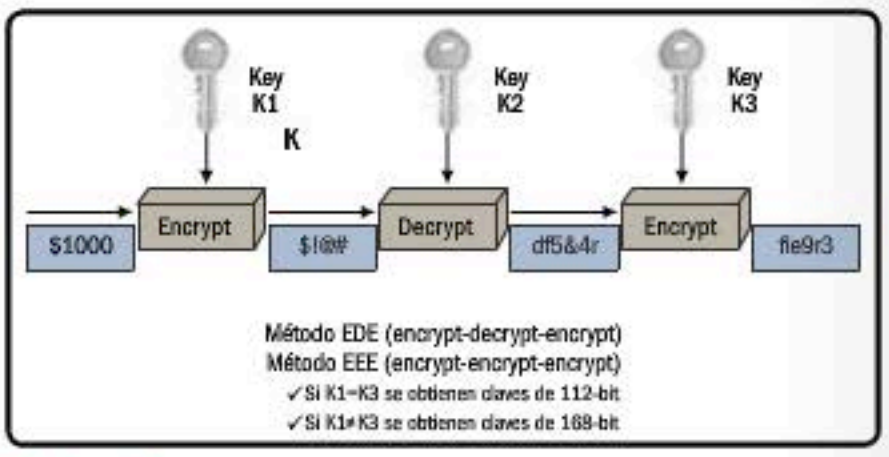


Figura 9. **Distintas implementaciones de la función 3DES.**

EL NOMBRE Y EL ALGORITMO

El nombre del algoritmo Rijndael es una palabra compuesta a partir de los nombres de sus creadores, aunque en rigor de verdad AES no es el algoritmo Rijndael puro sino una variación, similar a lo sucedido con DES y Lucifer.

IDEA

IDEA o International Data Encryption Algorithm es un cifrador por bloques diseñado por Xuejia Lai y James L. Massey de la Escuela Politécnica Federal de Zúrich en 1991. Previamente, en 1990, sus creadores habían desarrollado un algoritmo denominado **PES** (Proposed Encryption Standard). Poco tiempo después, debido a los avances en criptoanálisis diferencial alcanzados por Adi Shamir y Eli Biham, propusieron una mejora denominada **IPES** (Improved Proposed Encryption Standard) y, finalmente, IDEA como versión definitiva.

En 1999, demostrada su mayor fortaleza frente a otros algoritmos como DES y sus variantes, se comenzó a utilizar en **PGP** (Pretty Good Privacy) y otras aplicaciones. Si bien IDEA es libre para uso no comercial, fue patentado y registrado como marca por la compañía **MediaCrypt** y sus patentes vencieron en los años 2010 y 2011, respectivamente.

Además de su fortaleza, otro punto importante es que al ser un algoritmo europeo, nunca tuvo las limitaciones de exportación impuestas a los algoritmos americanos, lo que motivó que su adopción se realizar de una manera muy rápida. Respecto a la seguridad de este algoritmo, el ataque por fuerza bruta resulta impracticable computacionalmente.

Figura 10. TrueCrypt **es una herramienta libre para el cifrado de discos.**

AES

Tanto en 1987 como en 1993, el **NIST** volvió a certificar a DES. Durante estos años se estandarizó como algoritmo de cifrado en todo el mundo. Finalmente, en 1997 NIST no volvió a certificarlo y llamó a un concurso internacional para buscar un nuevo estándar mundial de cifrado denominado AES. Entre 1997 y 1999 el DES se enfrentó a tres desafíos conocidos como **DES Challenge**, que impulsa y promociona la compañía **RSA**.

En la última instancia de la competencia, para encontrar al reemplazo de DES quedaron cinco

EL MÉTODO KASISKI

Es un método de criptoanálisis aplicable al viejo cifrador de Vigenere desarrollado por Friedrich Kasiski que consiste en determinar la clave utilizada en este cifrador a partir de buscar palabras que se repitan dentro del texto cifrado.

algoritmos como finalistas, siendo el ganador uno de origen belga desarrollado por los ingenieros y criptógrafos Joan Daemen y Vincent Rijmen. Rijndael permite un mayor rango de tamaño de bloques y longitud de claves. AES tiene un tamaño de bloque fijo de 128 bits y claves de 128, 192 o 256 bits, mientras que Rijndael soporta claves múltiplo de 32 bits, con un mínimo de 128 bits y un máximo de 256 bits. Al contrario de su predecesor, no es una red de Feistel, sino una **red de sustitución-permutación**, conceptualmente similar a IDEA.

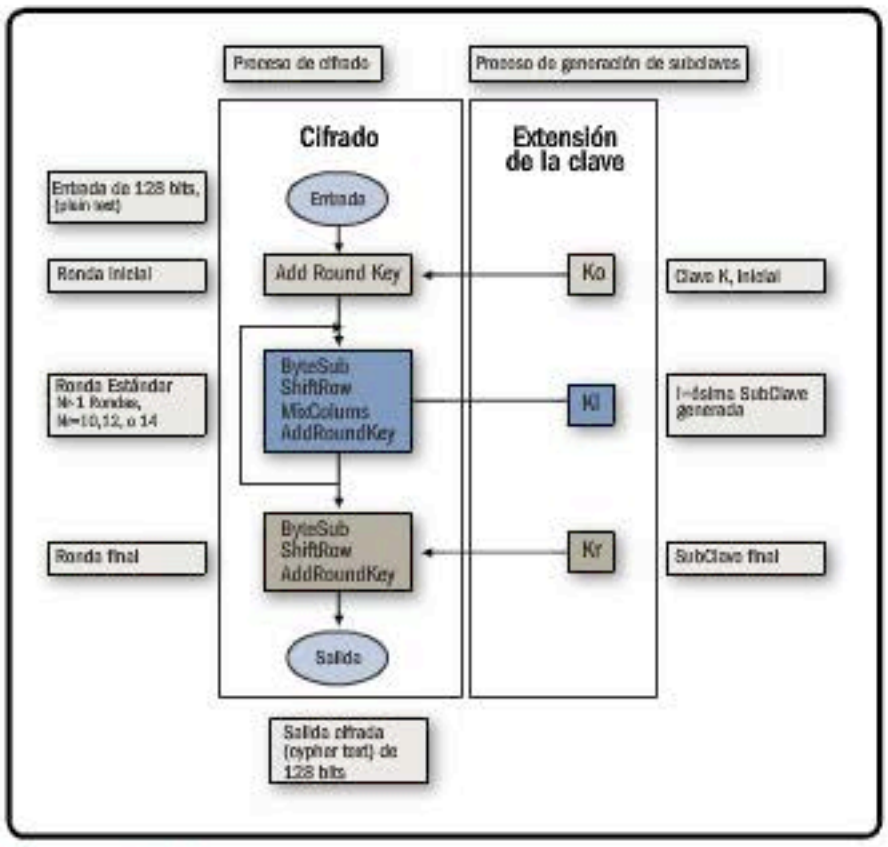


Figura 11. **Funciones utilizadas por AES dependiendo de la vuelta.**

Algoritmos **asimétricos**

Al comienzo de este capítulo mencionamos que, dependiendo de los algoritmos de cifrado, podríamos usar una o más claves para cifrar/descifrar un determinado dato. En el caso de los algoritmos simétricos, se utilizaba una misma clave para cifrar y descifrar, denominada clave secreta. En los algoritmos asimétricos o de clave pública, utilizaremos **dos claves**, una **pública** y una **privada**. Entonces, si ciframos con una, tenemos que descifrar con la otra.

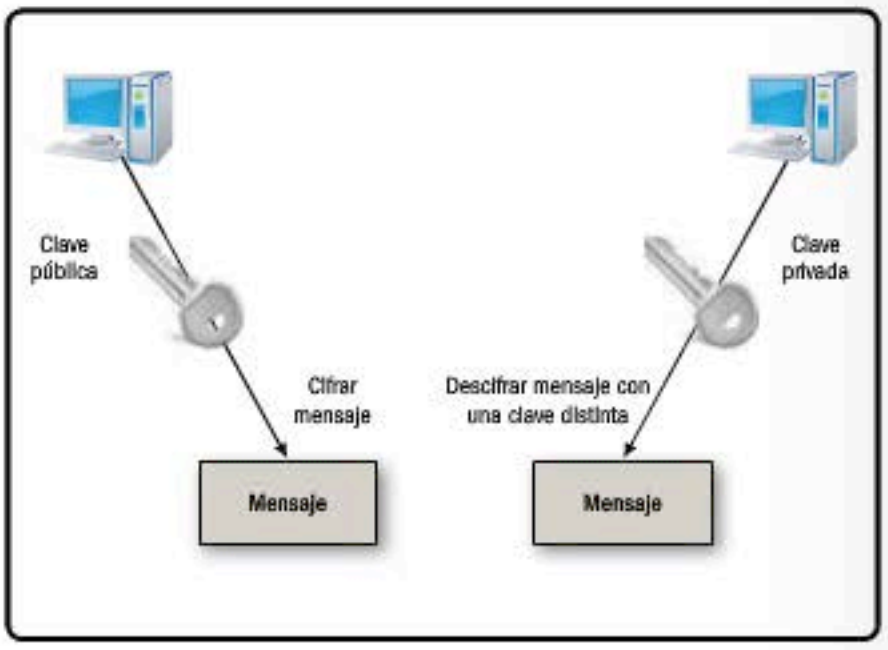


Figura 12. **En un algoritmo asimétrico, el cifrado y el descifrado utilizan claves distintas, se los llama** algoritmos de clave pública.

REFERENCIA RÁPIDA Y CONCEPTOS MATEMÁTICOS

Podemos obtener información sobre las funciones y operaciones matemáticas mencionadas en el capítulo consultando las entradas de Wikipedia en español: Teoría de números, Números primos, Operadores lógicos, Módulo matemático, Congruencia y Aritmética modular.

Típicamente, utilizamos estos algoritmos para el **intercambio** de claves y la **firma digital**. En el primer caso, dado que el cifrado asimétrico es mucho más lento que el cifrado simétrico, estos se centran en distribuir las claves para cifrar con un algoritmo simétrico entre dos extremos que se quieren comunicar. Esto se hace cifrando pequeñas cantidades de información, por ejemplo, una clave de 128 o 256 bits. En el caso de la firma digital, se busca **autenticar** y además garantizar el **no repudio**. Recordemos que este requerimiento de seguridad garantiza que un usuario no pueda negar que realizó una determinada acción. Por ejemplo, en una transacción comercial efectuada a través de Internet.

Figura 13. La firma digital se utiliza para garantizar la autenticidad y la integridad en diversos documentos.

RSA

Este algoritmo fue desarrollado, en 1977, por Ron Rivest, Adi Shamir y Len Adleman en el **MIT**. Las letras **RSA** son las iniciales de sus apellidos y fue patentado por el MIT en 1983, patente que expiró el 21 de septiembre de 2000. RSA brinda posibilidades de cifrado, intercambio de llaves y autenticación.

Figura 14. Podemos visitar el sitio oficial de la RSA Security en www.rsa.com.

Dado que los algoritmos asimétricos son mucho más **lentos** que los simétricos, lo que se busca cifrar son datos pequeños, por ejemplo, la clave secreta que se utilizaría para cifrar/descifrar un mensaje en ambos extremos. Esto es así ya que la complejidad matemática

PARADOJA DEL CUMPLEAÑOS

Esta paradoja se basa en cálculos con los que se puede demostrar que la probabilidad de colisiones en un algoritmo de hash es mayor que lo esperados. Se la llama así porque se ejemplifica con la probabilidad de que dos personas cumplan años el mismo día.

utilizada en los algoritmos asimétricos es mucho mayor que la que se utiliza en sus pares simétricos (basados en el procesamiento de matrices).

Actualmente, el tamaño típico de las claves es de 1024 o 2048 bits, pero se pueden alcanzar los 4096 y 8192 bits.

DIFFIE-HELLMAN

Es un algoritmo desarrollado por Whitfield Diffie y Martin Hellman que fue publicado en 1976. En rigor de la verdad, **Diffie-Hellman (DH)** es solamente un **protocolo de intercambio de claves**, ya que no permite cifrado ni firma como sí lo hace RSA.

Una ventaja de DH es que la llave nunca se envía por el canal. Solo se envían una serie de parámetros a través de los cuales, utilizando funciones matemáticas, ambos extremos pueden **reconstruir una clave** compartida. La seguridad radica en la complejidad de calcular **logaritmos discretos**, incluso más difícil que el cálculo de los números primos grandes utilizados en RSA. En la figura 15 podemos ver los parámetros que utiliza esta función y qué transmite cada una de las partes.

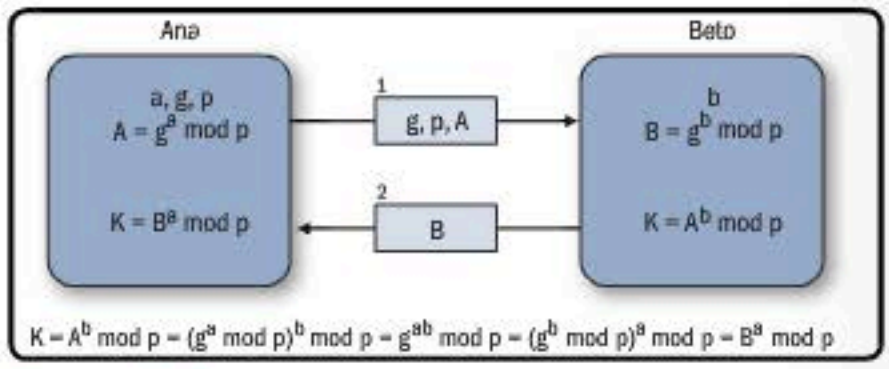


Figura 15. Parámetros del algoritmo Diffie-Hellman e intercambio para regenerar la clave en cada extremo.

DH es susceptible de sufrir ataques del tipo **MITM** (man-in-the-middle). Suponiendo que la comunicación es interceptada por un atacante, este podría, por ejemplo, hacerle creer a Beto que él es Ana y viceversa, ya que no se autentica en primera instancia. De esta forma, el atacante podría intercambiar claves con Beto por un lado, pudiendo finalmente escuchar la conversación en ambos sentidos. Para solucionar esto, junto con DH se utiliza el algoritmo **DSA** de firma digital, garantizando de este modo la identidad de cada una de las partes.

ELGAMAL

Este algoritmo, publicado en 1985 por Taher ElGamal, extiende los conceptos matemáticos de DH con el objeto de soportar un criptosistema completo de clave pública, es decir, con la implementación de **ElGamal** es posible obtener **firma**

ALGORITMOS Y ESTÁNDARES

Información relativa a los algoritmos criptográficos que constituyen estándares internacionales puede obtenerse en sitios web de las distintas organizaciones como: IETF (www.ietr.org), ISO (www.iso.org), IEC (www.iec.org) y NIST (www.nist.gov).

digital y cifrado. A diferencia de RSA, ElGamal no fue patentado, por lo que es de dominio público.

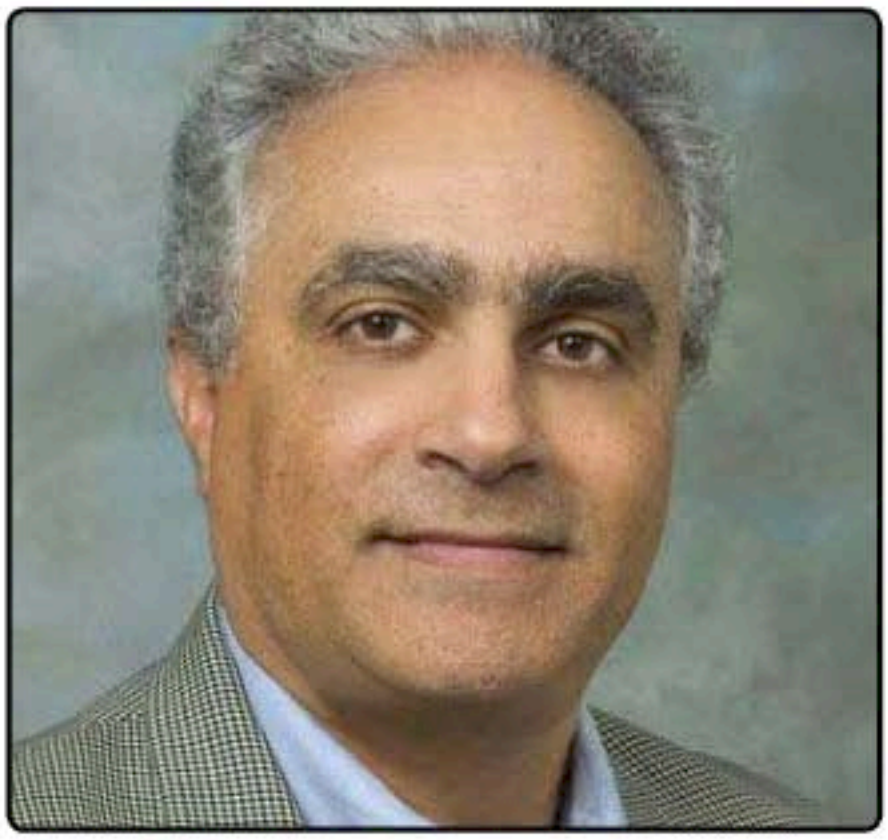


Figura 16. El doctor Taher ElGamal es el creador del algoritmo de cifrado asimétrico, que lleva su nombre.

La seguridad del algoritmo está basada en el mismo supuesto matemático que DH: el **PLD (Problema del Logaritmo Discreto)**. El esquema de funcionamiento básico de ElGamal consta de tres componentes: el **generador de claves**, el **algoritmo de cifrado** y el de **descifrado**. A continuación, describimos el funcionamiento del algoritmo.

Con respecto a la **seguridad**, hasta el momento el algoritmo ElGamal es considerado un algoritmo efectivo: solo podría romperse si el atacante es capaz de calcular logaritmos discretos. Sin embargo, en la actualidad no existen algoritmos eficientes para realizar este cálculo en un tiempo razonable. En el momento de la implementación, existe un caso en el que este algoritmo se vuelve maleable. Esto implica que en ciertas condiciones, la seguridad de ElGamal puede comprometerse. Este ataque considera que el atacante tiene el criptograma y el mensaje conocido. Si el emisor que cifró el mensaje anterior genera un nuevo mensaje cifrado utilizando la misma clave privada, el atacante podría obtener el nuevo mensaje en texto plano.

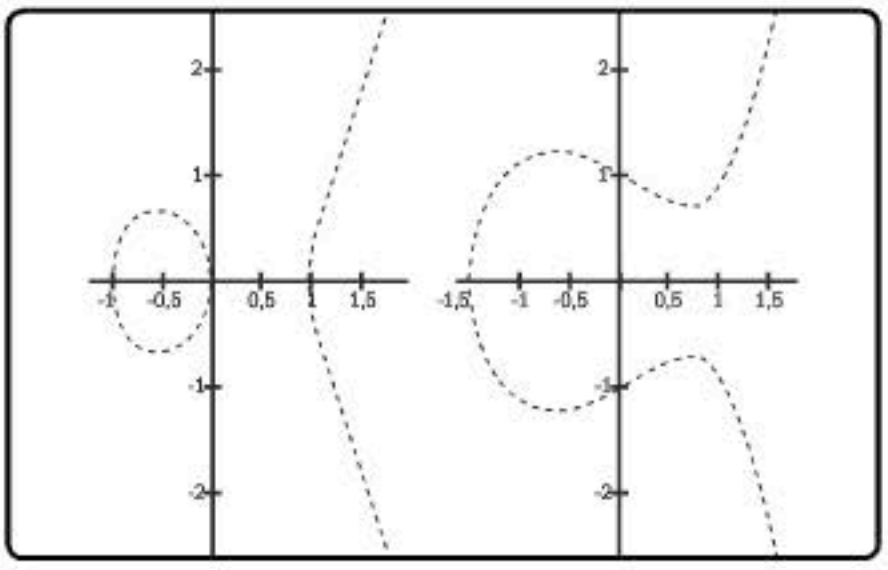


Figura 17. El cifrado de curvas elípticas definidas por su ecuación característica en que se basa la generación de claves.

LECTURAS COMPLEMENTARIAS

Si bien el tema de criptografía puede ser arduo de entender, existen excelentes escritos, como: Applied Cryptography de Bruce Scheneir, Cryptography & Network Security de William Stallings y Teoría de la Información de Claude Shannon.

Funciones
Hash

La informática define como **función hash** a un algoritmo que permite generar **resúmenes** que representen de manera cuasi unívoca a un archivo o dato. También se le da el nombre de **hash** o **digest** al resultado de esa función. Estas funciones identifican probabilísticamente a un conjunto de información, dando como resultado un conjunto imagen de tamaño fijo, generalmente menor. Su propiedad fundamental es que si dos resultados de una misma función son diferentes, las entradas que generaron esos resultados también lo son. No obstante, al ser mucho menor el rango posible de claves que el rango posible de objetos, pueden existir claves resultantes iguales para objetos diferentes, hecho conocido como **colisiones**.

Un ejemplo es MD5, desarrollado por Ron Rivest en 1992 y basado en sus predecesores **MD4** y **MD2** a los que se les realizaron mejoras, dando lugar a un algoritmo más seguro, pero más lento. Los resúmenes resultantes son de **128 bits**. Desde 2005 ha quedado obsoleto debido a que los estudiantes Xiaoyun Wang, Dengguo Feng, Xuejia Lai y Hongbo Yu de la **Shandong University** (China) anunciaron el descubrimiento de **colisiones de hash** para esta función. Si bien en ese momento el ataque solo fue teórico y con un cluster armado para tal fin, más tarde se pudo llevar a cabo en forma práctica. Aun así, sigue siendo un algoritmo interesante debido a su sencillez y generalidad.

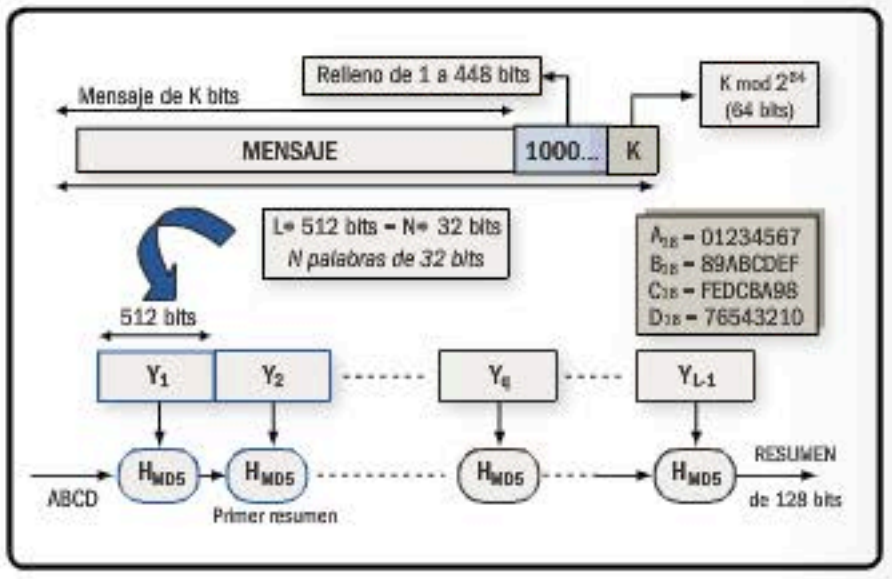
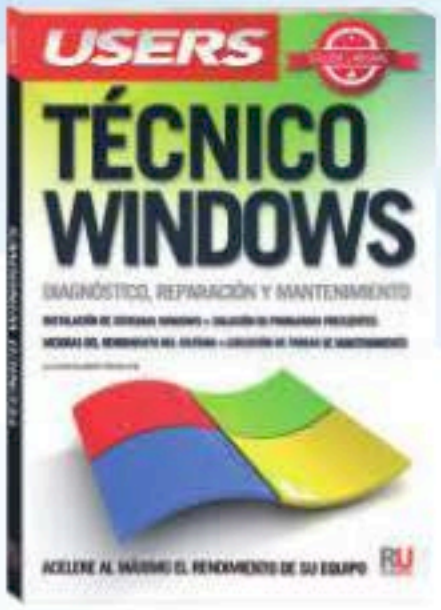


Figura 18. Esquema de funcionamiento genérico de la función MD5.

Otro de los más utilizados es SHA, cuya versión más utilizada y actual estándar es **SHA-1**, desarrollada en 1994. La familia SHA fue desarrollada por la **NSA** (National Security Agency) y, actualmente, existen cuatro variantes denominadas **SHA-2** (SHA-224, SHA-256, SHA-384 y SHA-512). SHA-1 es similar en funcionamiento a MD5, pero genera un resumen de **160 bits**.

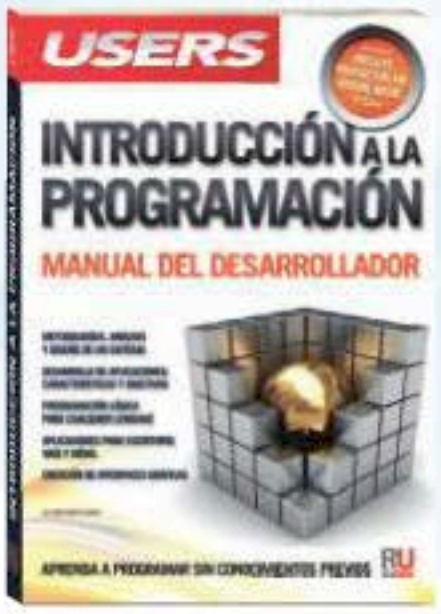
RESUMEN

En este capítulo tratamos los aspectos principales de la criptografía. Presentamos los distintos tipos de algoritmos, las funciones de hash y los sistemas criptográficos. Analizamos el concepto de infraestructura de clave pública, las aplicaciones de la criptografía y los diferentes tipos de ataques a criptosistemas.



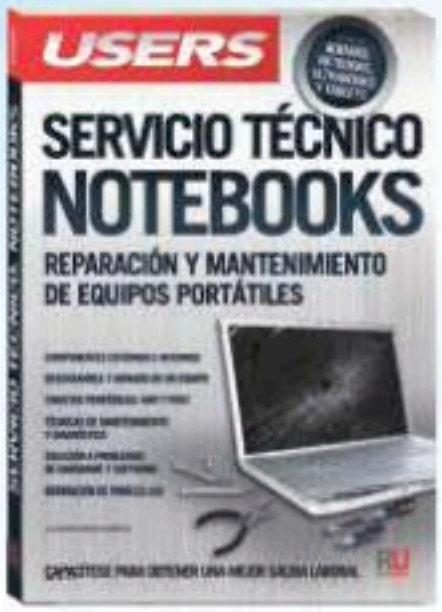
Esta obra reúne todos los conocimientos teóricos y prácticos para convertirse en un técnico especializado en Windows.

→ 320 páginas / ISBN 978-987-1857-70-8



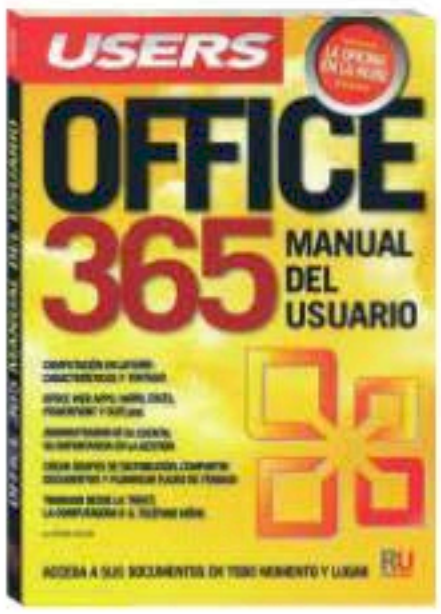
Libro ideal para iniciarse en el mundo de la programación y conocer las bases necesarias para generar su primer software.

→ 384 páginas / ISBN 978-987-1857-69-2



Presentamos una obra fundamental para aprender sobre la arquitectura física y el funcionamiento de los equipos portátiles.

→ 352 páginas / ISBN 978-987-1857-68-5

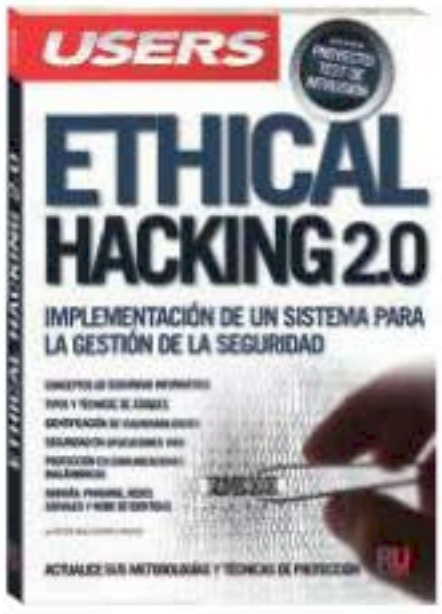


Una obra ideal para aprender todas las ventajas y servicios integrados que ofrece Office 365 para optimizar nuestro trabajo.

→ 320 páginas / ISBN 978-987-1857-65-4

Esta obra presenta las mejores aplicaciones y servicios en línea para aprovechar al máximo su PC y dispositivos multimedia.

→ 320 páginas / ISBN 978-987-1857-65-4



Esta obra va dirigida a todos aquellos que quieran conocer o profundizar sobre las técnicas y herramientas de los hackers.

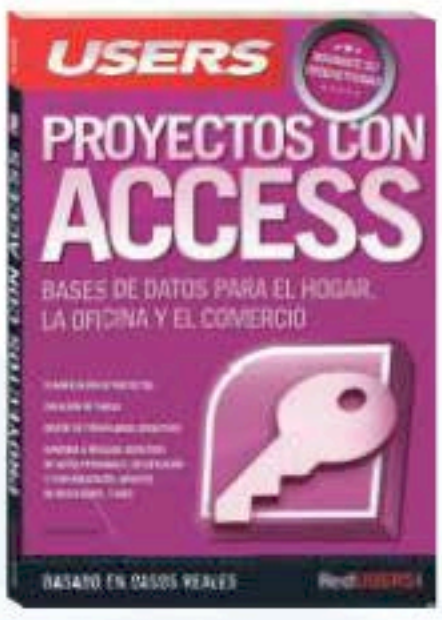
→ 352 páginas / ISBN 978-987-1857-63-0

Este libro se dirige a fotógrafos amateurs, aficionados y a todos aquellos que quieran perfeccionarse en la fotografía digital.

→ 352 páginas / ISBN 978-987-1857-48-7

En este libro encontraremos una completa guía aplicada a la instalación y configuración de redes pequeñas y medianas.

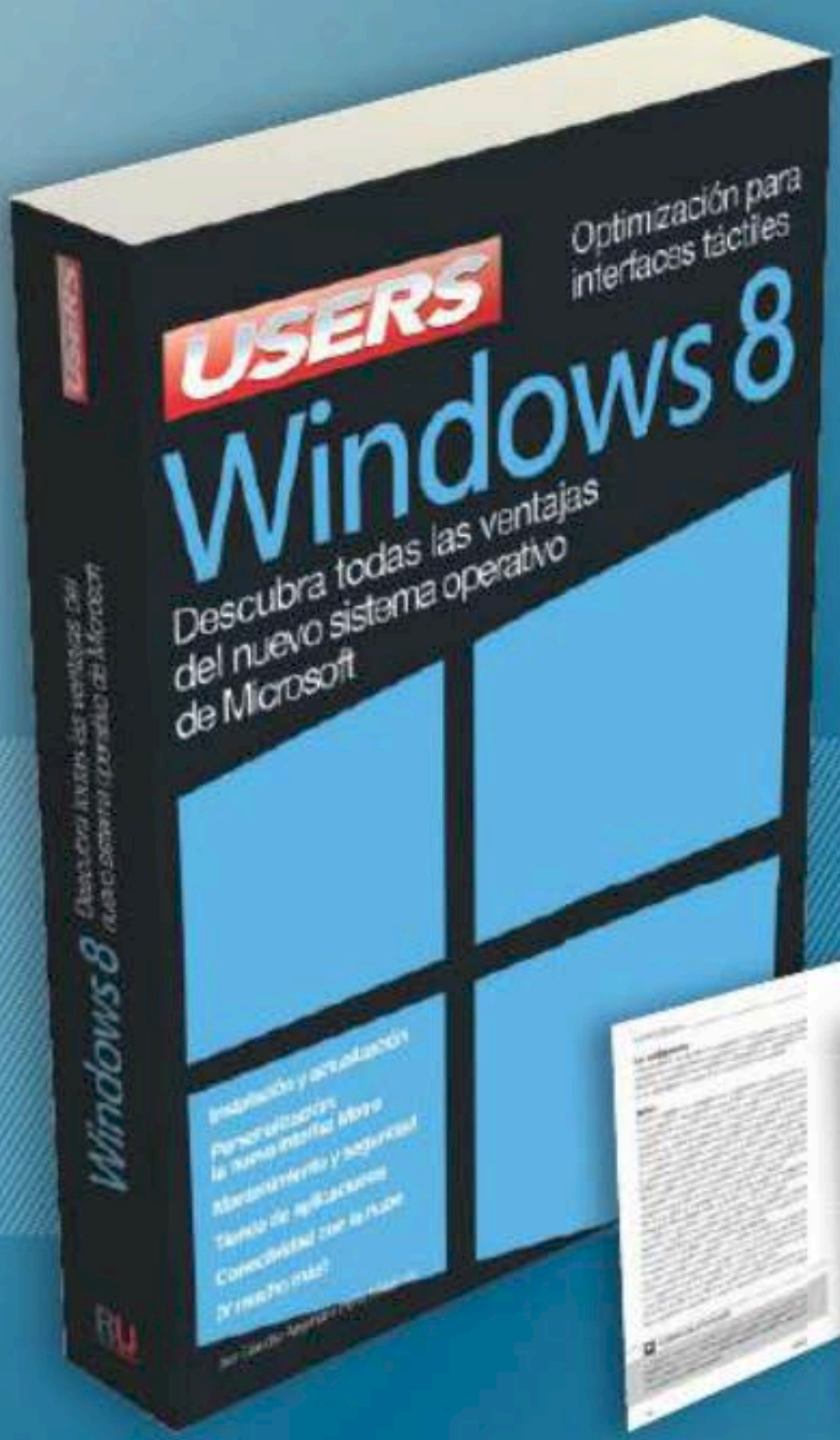
→ 320 páginas / ISBN 978-987-1857-46-3



Esta obra está dirigida a todos aquellos que buscan ampliar sus conocimientos sobre Access.

→ 320 páginas / ISBN 978-987-1857-45-6

DESCUBRA TODAS LAS VENTAJAS DEL NUEVO SISTEMA OPERATIVO DE MICROSOFT



Luego del lanzamiento de un sistema operativo sólido y veloz como Windows 7, Microsoft ha desarrollado un nuevo sistema que presenta una interfaz renovada, disponible tanto para equipos de escritorio y portátiles, como para tablets. Esta obra nos permitirá descubrir esta novedad, junto a otros aspectos en términos de seguridad y rendimiento, para aprovechar el potencial de Windows 8 al máximo.

» MICROSOFT / WINDOWS
» 192 PÁGINAS
» ISBN 978-987-1857-67-8

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

+54 (011) 4110-8700

USERS

Técnico en
REDES &SEGURIDAD

ETHICAL HACKING

CONTENIDO

La presente obra expone conocimientos imprescindibles para el usuario acerca de las técnicas de seguridad existentes. Informa sobre las vulnerabilidades frecuentes y los accesos al sistema, y advierte sobre los errores más comunes cometidos con frecuencia al aplicar seguridad. Además, lista de manera clara y didáctica una clasificación sobre los diferentes tipos de hackers, e informa sobre sus ataques a nivel individual y masivo. Aborda también indispensables cuestiones de seguridad física e ingeniería social.

EXCLUSIVO PARA LECTORES

Profesores en línea:
profesor@redusers.com

Servicios para lectores:
usershop@redusers.com

9 789871 857753