

Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Analista de Seguridad Informática



Organiza



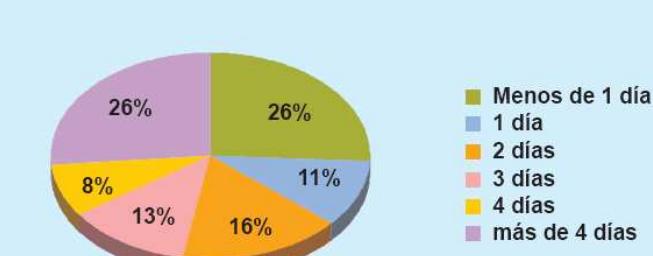
Enseñanzas Propias



Dpto. Lenguajes y Computación

Julio Gómez López

¿Cuánto tiempo estima que puede sobrevivir su empresa sin la información contenida en los ordenadores?



Fuente: AEDI política empresarial de la seguridad

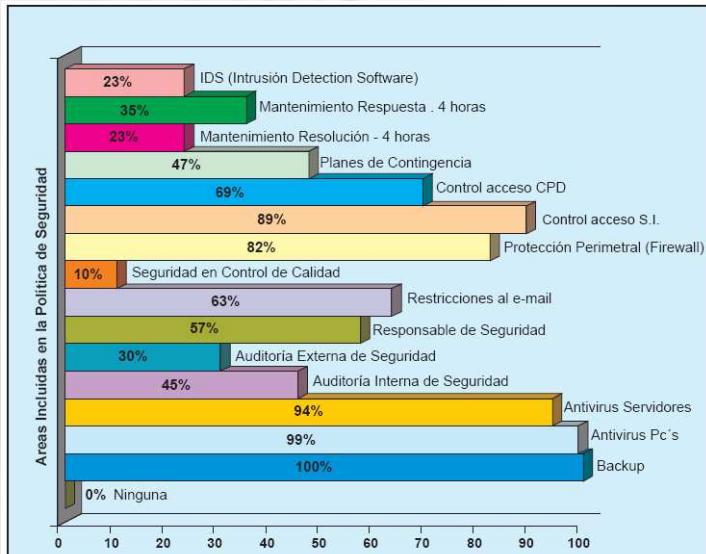


© Julio Gómez López jgomez@ual.es
www.administraciondesistemasoperativos.com
Universidad de Almería

Analista de Seguridad Informática

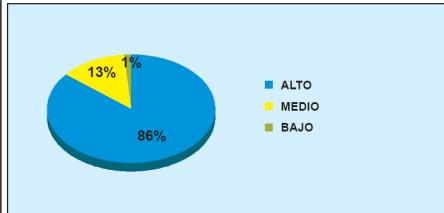
Capítulo 1. Conceptos básicos

¿Qué áreas se incluyen en la política de seguridad de la empresa?

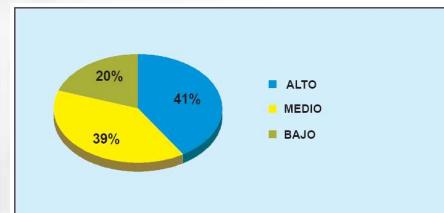


Fuente: AEDI política empresarial de la seguridad

¿Cuál es el grado de preocupación de responsable de la dirección de informática sobre la seguridad?



¿Cuál es el grado de preocupación de responsable de la dirección general sobre la seguridad?

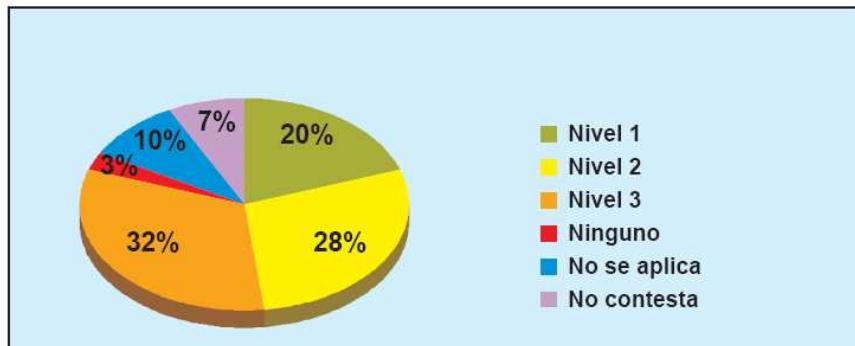


Fuente: AEDI política empresarial de la seguridad

Analista de Seguridad Informática

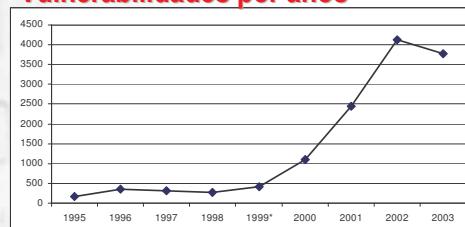
Capítulo 1. Conceptos básicos

¿Cuál es el máximo nivel de Seguridad para su empresa respecto a la LOPD?



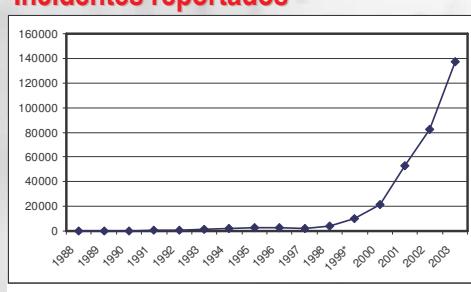
Fuente: AEDI política empresarial de la seguridad

Vulnerabilidades por años



Data Source: CERT (<http://www.cert.org>)

Incidentes reportados



Data Source: CERT <http://www.cert.org>



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Kevin D. Mitnick



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Kevin D. Mitnick

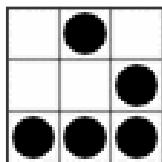
The screenshot shows the homepage of Kevin D. Mitnick's security consulting firm. It includes a sidebar for a speaking schedule, a section for getting his business card, and a prominent advertisement for his book 'El Arte de la Intrusión'.

The screenshot displays a news article from the website ideal.es. The headline reads: 'Un 'hacker' burla la seguridad informática en la facultad y roba datos de alumnos y profesores'. The article discusses a security breach at the University of Granada where a hacker accessed student and professor data. It includes a photo of students working on computers and a sidebar for online shopping.



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos



El juego de la vida

[...]

Ahora este es nuestro mundo . . .

El mundo del electrón y el conmutador, la belleza del baudio.

Nosotros hacemos uso de un servicio que ya existe sin pagar por lo que podría ser barato como el polvo, si no estuviera en manos de glotones hambrientos de ganancias,

y ustedes nos llaman criminales.

Nosotros exploramos . . .

y ustedes nos llaman criminales.

Nosotros buscamos detrás del conocimiento . . .

y ustedes nos llaman criminales.

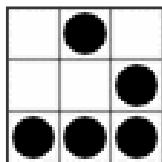
Nosotros existimos sin color, sin nacionalidad, sin prejuicios religiosos . . .

y ustedes nos llaman criminales.

Ustedes construyeron bombas atómicas,

ustedes hicieron la guerra,

ustedes asesinaron, engañaron y nos mintieron
y trajeron de hacernos creer que era por nuestro bien,
ahora nosotros somos los criminales.



El juego de la vida

[...]

Si, soy un criminal.

Mi crimen es la curiosidad.

Mi crimen es el juzgar a las personas por lo que dicen y piensan,
no por lo que aparentan.

Mi crimen es ser más inteligente, algo por lo cual nunca me olvidarás.

Soy un Hacker, este es mi manifiesto.

Tu podrás detener este esfuerzo individual, pero nunca podrás detenernos a todos

...

después de todo, todos somos iguales.

[...]

Extracto de texto del Manifiesto de un Hacker



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

	Capítulo 1. Conceptos básicos
Contenido	
Presentación	
Definiciones	
Tipos de ataques	



Presentación

	Capítulo 1. Conceptos básicos
Contenido	
Presentación	CAPÍTULO 1 CONCEPTOS BÁSICOS
Definiciones	1 Amenazas de seguridad
Tipos de ataques	2 Tipos de ataques
	CAPÍTULO 2 BUSCAR UN VECTOR DE ATAQUE
	1 Localizar el objetivo
	2 Analizar el objetivo
	CAPÍTULO 3. ANALISTA DE SISTEMAS
	1 Introducción
	2 Escaneo de vulnerabilidades
	3 Explotar las vulnerabilidades del sistema (metasploit)
	4 Ataques contra contraseñas de los usuarios



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Capítulo 1. Conceptos básicos	
Contenido	
Presentación	CAPÍTULO 4. ANALISTA DE REDES
Definiciones	1 Introducción
Tipos de ataques	2 Man in the middle
	3 Sniffers
	4 Técnicas de ocultación y navegación anónima (torpak)
	CAPÍTULO 5. ANALISTA DE SERVIDORES WEB
	1 Introducción
	2 Búsqueda de vulnerabilidades
	3 XSS (Cross Site Scripting)
	4 Remote File Inclusión (RFI)
	5 Inyección de SQL

Capítulo 1. Conceptos básicos	
Contenido	
Presentación	CAPÍTULO 6. ANALISTA DE APLICACIONES
Definiciones	1 Introducción
Tipos de ataques	2 Crack
	3 Troyanizando netcat
	4 KeyLoggers
	5 Troyanos
	6 Ocultación para el antivirus



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Capítulo 1. Conceptos básicos	
Contenido	CAPÍTULO 1. CONCEPTOS BÁSICOS 1 Amenazas de seguridad 2 Tipos de ataques
Presentación	CAPÍTULO 2. BUSCAR UN VECTOR DE ATAQUE 1 Localizar el objetivo 2 Analizar el objetivo
Definiciones	CAPÍTULO 3. ANALISTA DE SISTEMAS 1 Introducción 2 Escaneo de vulnerabilidades 3 Explorar las vulnerabilidades del sistema (metasploit) 4 Ataques contra contraseñas de los usuarios
Tipos de ataques	Exploits Analizar sistemas Romper contraseñas
	CAPÍTULO 4. ANALISTA DE REDES 1 Introducción 2 Man in the middle 3 Sniffers 4 Técnicas de ocultación y navegación anónima (torpak)
	Sniffers -- phising Man in the middle DoS -- ocultación
	CAPÍTULO 5. ANALISTA DE SERVIDORES WEB 1 Introducción 2 Búsqueda de vulnerabilidades 3 XSS (Cross Site Scripting) 4 Remote File Inclusion (RFI) 5 Inyección de SQL
	XSS SQL injection RFI
	CAPÍTULO 6. ANALISTA DE APLICACIONES 1 Introducción 2 Crack 3 Troyanizando netcat 4 KeyLoggers 5 Troyanos 6 Ocultación para el antivirus
	Crack Keyloggers Troyanos Ocultación Virus

www.administraciondesistemasoperativos.com

INSCRIBITE YA

moodle

Bienvenido a la plataforma de enseñanza virtual del portal de Administración de Sistemas Operativos.

Contraseña: backtrack



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Calendario

Febrero

L	M	X	J	V	S	D
18	19	20	21	22	23	24
25	26	27	28	29		

Marzo

L	M	X	J	V	S	D
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23

Examen

Entrega de actas

Día 1- básico	Día 2 – red	Día 3 – web	Día 4 -web	Día 5 -sql	Día 6 - aplicaciones
Presentación Conceptos básicos SAM /john	Man in the middle DNS / phising / sniffer	Búsqueda	RFI	Crack	Keyloggers Troyanos
Metasploit VNC/W2k3	Sniffer VoIP Ocultación	XSS	SQL inyection	Troyanizando netcat	Ocultación de virus Examen



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Metodología



RETO

Los retos permiten que el alumno pueda poner a prueba sus conocimientos



CONTRAMEDIDAS

Se explica la forma de mitigar un determinado ataque

IMPORTANTE

El único objetivo del curso es que el alumno sea capaz de auditar sistemas informáticos que se encuentran bajo su responsabilidad.

El alumno es el único responsable si utiliza los conocimientos para entrar en sistemas sin permiso.



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

	Capítulo 1. Conceptos básicos
Contenido	
Presentación	
Definiciones	
Tipos de ataques	



Definiciones

	Capítulo 1. Conceptos básicos
Contenido	
Presentación	
Definiciones	Analista informático
Tipos de ataques	<p>Disciplina que se refiere al análisis de las condiciones de una instalación informática por un auditor externo e independiente que realiza un dictamen sobre diferentes aspectos.</p> <p>Conjunto de procedimientos y técnicas para evaluar y controlar, total o parcialmente, un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente.</p>



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Capítulo 1. Conceptos básicos	
Contenido	Hacker
Presentación	
Definiciones	
Tipos de ataques	
	<p>Hacker [originalmente, alguien que fabrica muebles con un hacha] n.</p> <p>1. Persona que disfruta con la exploración de los detalles de los sistemas programables y cómo aprovechar sus posibilidades; al contrario que la mayoría de los usuarios, que prefieren aprender sólo lo imprescindible. 2. El que programa de forma entusiasta (incluso obsesiva). 3. Persona capaz de apreciar el valor del hackeo. 4. Persona que es buena programando de forma rápida. 5. Experto en un programa en particular, o que realiza trabajo frecuentemente usando cierto programa; como en «es un hacker de Unix.» (Las definiciones 1 a 5 están correlacionadas, y la gente que encaja en ellas suele congregarse.) 6. Experto o entusiasta de cualquier tipo. Se puede ser un «hacker astrónomo», por ejemplo. 7. El que disfruta del reto intelectual de superar o rodear las limitaciones de forma creativa. 8 [en desuso] Liante malicioso que intenta descubrir información sensible cotilleando por ahí. De ahí vienen «hacker de contraseñas» y «hacker de las redes». El término correcto en estos casos es cracker.</p>

Capítulo 1. Conceptos básicos	
Contenido	Hacker
Presentación	
Definiciones	
Tipos de ataques	
	<p>En palabras del gurú informático Richard Stallman, “un hacker puede ser aquel que se divierte empleando al máximo su inteligencia, sin la necesidad de ocasionar daños a un tercero”. Aunque, actualmente, el alcance de la actividad de los “piratas informáticos” excede los límites del simple ocio y la recreación.</p> 



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Capítulo 1. Conceptos básicos	
Contenido	
Presentación Definiciones Tipos de ataques	<p>Cracker</p> <p>Cracker n. El que rompe la seguridad de un sistema. Acuñado hacia 1985 por hackers en defensa ante la utilización inapropiada por periodistas del término hacker (en su acepción número</p>

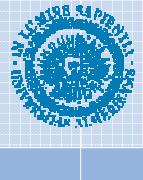
Capítulo 1. Conceptos básicos	
Contenido	
Presentación Definiciones Tipos de ataques	<p>Ética de un hacker (I)</p> <p>Esta es (o era) la definición original de la ética del hacker:</p> <ul style="list-style-type: none">•El acceso a los ordenadores, y a cualquier cosa que pudiera enseñarte algo sobre cómo funciona el mundo debería ser ilimitado y total•Básate siempre en el imperativo de la práctica•Toda información debería ser libre•Desconfía de la autoridad, promueve la descentralización•Los hackers deberían ser juzgados únicamente por su habilidad en el hackeo, no por criterios sin sentido como los títulos, edad, raza o posición social•Se puede crear arte en un ordenador•Los ordenadores pueden cambiar tu vida a mejor



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

	<h3>Capítulo 1. Conceptos básicos</h3>
Contenido Presentación Definiciones Tipos de ataques 	<h4>Ética de un hacker (II)</h4> <p>Estas son otras definiciones y/o «sentidos» de la Ética del Hacker, actualizadas (¿simplificadas? ¿mejores? ¿más del siglo XXI y del software libre?):</p> <ul style="list-style-type: none">•La creencia en que compartir información es un bien poderoso y positivo, y que es tarea ética de los hackers compartir sus experiencias escribiendo código abierto («open source») y facilitando el acceso a la información y los recursos de computación siempre que sea posible•La creencia de que romper sistemas por diversión y exploración está éticamente bien siempre que el cracker no cometa un robo, un acto de vandalismo o vulnere la confidencialidad

	<h3>Capítulo 1. Conceptos básicos</h3>
Contenido Presentación Definiciones Tipos de ataques 	<h4>Phreakers</h4> <p>Un phreaker es una persona que investiga los sistemas telefónicos, mediante el uso de tecnología por el placer de manipular un sistema tecnológicamente complejo y en ocasiones también para poder obtener algún tipo de beneficio como llamadas gratuitas.</p> 

Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Contenido

- Presentación
- Definiciones
- Tipos de ataques

Capítulo 1. Conceptos básicos

Tipos de ataques

Contenido

- Presentación
- Definiciones
- Tipos de ataques

Capítulo 1. Conceptos básicos

Tipos de ataques

Activos

Interrupción

The diagram shows a single node connected to a vertical bar with an arrow pointing right, representing an active attack that disrupts the flow of information.

Pasivos

Intercepción

The diagram shows two nodes connected by a horizontal line, with an arrow pointing from the first node to the second, and another arrow pointing down from the second node to a third node, representing an active attack that intercepts data without modifying it.

Modificación

The diagram shows two nodes connected by a curved line that loops back to the first node, representing an active attack that changes the data being transmitted.

Fabricación

The diagram shows two nodes connected by a curved line that loops back to the second node, representing an active attack that creates new data or messages.

Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Contenido

- Presentación
- Definiciones
- Tipos de ataques

Capítulo 1. Conceptos básicos

Grado de sofisticación

Figure 1. Attack Sophistication vs. Intruder Technical Knowledge

The graph illustrates the relationship between intruder knowledge and attack sophistication over time. The Y-axis represents 'Intruder Knowledge' (High to Low) and the X-axis represents 'Attack Sophistication' (Low to High). A curve shows the increasing complexity of attacks over time. Various attack types are plotted along the curve, including packet spoofing, denial of service, distributed attack tools, and 'stealth' techniques.

1980 1985 1990 1995 2000

Intruder Knowledge

Attack Sophistication

Tools

High

Low

Attackers

Contenido

- Presentación
- Definiciones
- Tipos de ataques

Capítulo 1. Conceptos básicos

Ataques

Sniffing

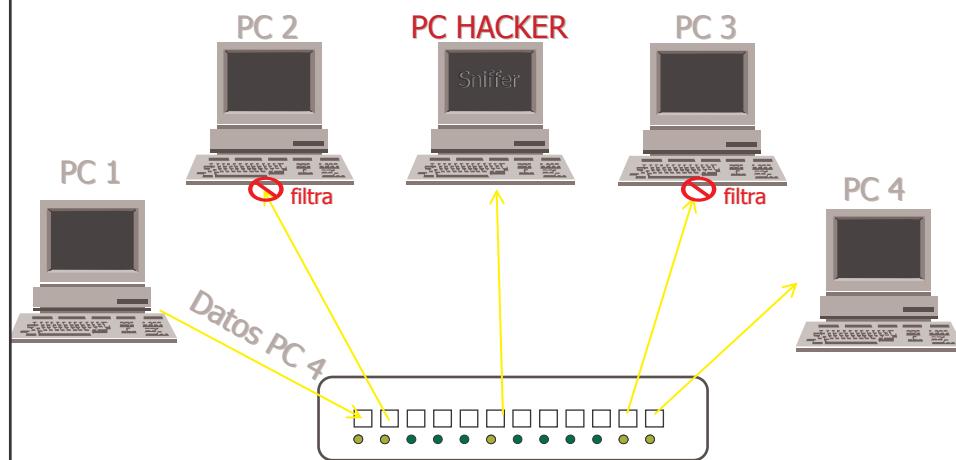
The screenshot shows the Abinet SessionWall 3 software interface. The main window displays a timeline of network events with detailed logs. The left sidebar shows icons for Mi PC, Internet Explorer, and other system components. The software is used for monitoring and analyzing network traffic.

Protección: Encriptado de datos (SSH). Servicios de Autentificación y auditoría

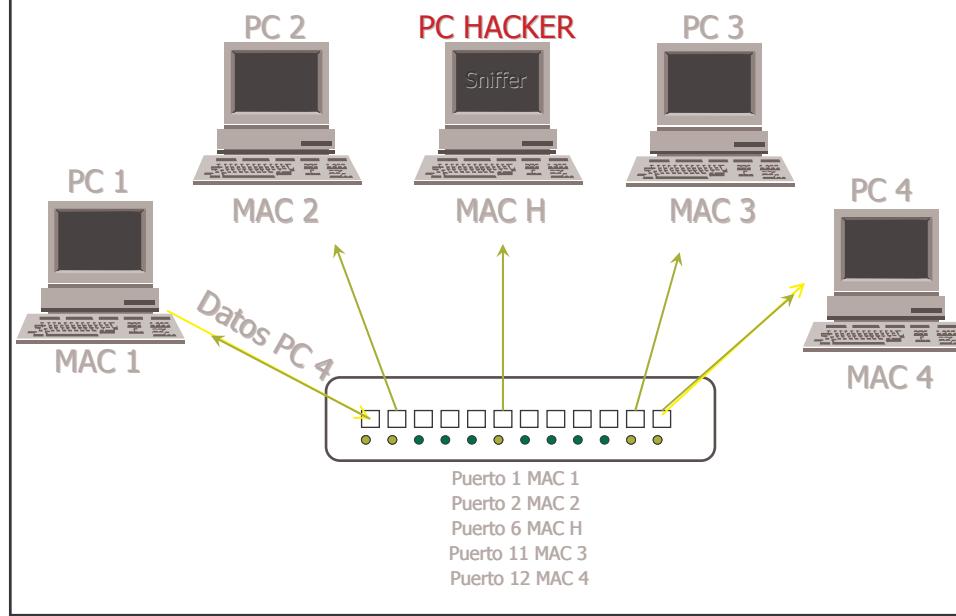
Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Sniffing (HUB)



Sniffing (Redes conmutadas Switch)



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Contenido

- Presentación
- Definiciones
- Tipos de ataques

Capítulo 1. Conceptos básicos

Ataques

Spoofing

El atacante envía paquetes con una dirección fuente incorrecta. Las respuestas se envían a la dirección fuente aparente y no al atacante.

Origen: Falso atacante
Destino: Objetivo atacado

Atacante

Atacado

Falso atacante

Contenido

- Presentación
- Definiciones
- Tipos de ataques

Capítulo 1. Conceptos básicos

Ataques

Spoofing

Puede utilizarse para: Ataque de Denegación de Servicio (DOS)

Origen: Objetivo atacado
Destino: Mensaje BroadCast

Atacante

Atacado

Falso atacante

Falso atacante

Falso atacante

Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

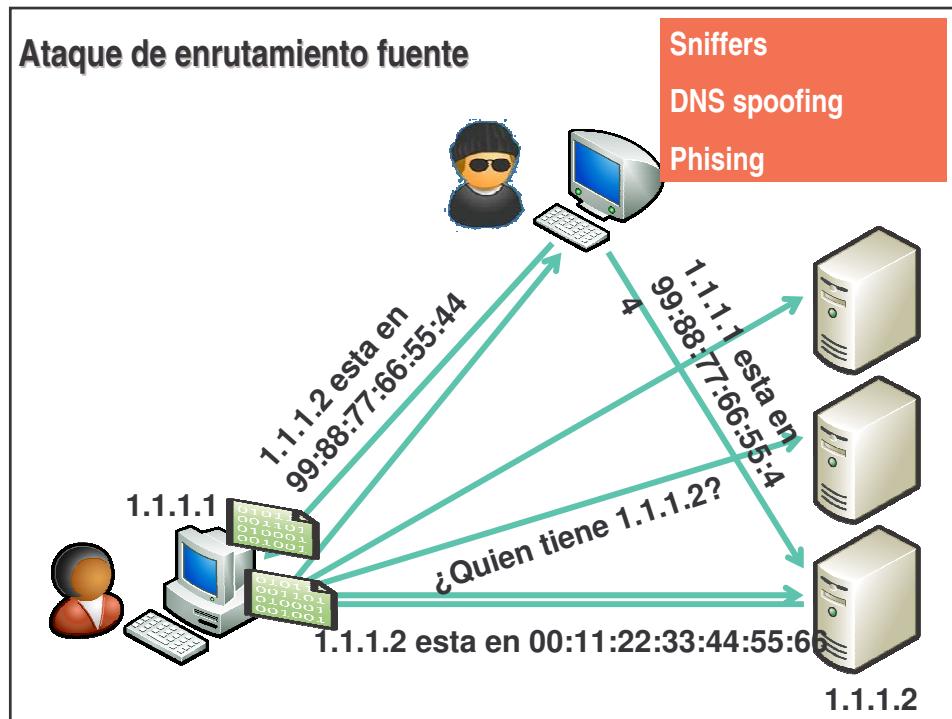
Contenido Presentación Definiciones Tipos de ataques	<h3>Capítulo 1. Conceptos básicos</h3> <h4>Spoofing</h4> <p>Puede utilizarse para: Ataque de Denegación de Servicio (DOS)</p>  <p>Atacante</p> <p>Atacado</p> <p>Origen: Objetivo atacado Destino: Objetivo atacado</p> <p>Origen: Objetivo atacado Destino: Objetivo atacado</p>
---	--

Contenido Presentación Definiciones Tipos de ataques	<h3>Capítulo 1. Conceptos básicos</h3> <h4>Enrutamiento fuente</h4> <p>Un atacante que controle un router entre origen y destino es capáz de cambiar un paquete que pase por el router.</p> <p>Un paquete de ida puede utilizar una ruta diferente a la de vuelta. Si en la idea pasa por un router comprometido, el atacante puede ver los paquetes.</p> <p>Protección: Filtrado de paquetes y encriptación</p>
---	---

	<h4>Mensajes de control de red</h4> <p>Utilizar un mensaje ICMP (redirect o destination unreachable) para hacer pasar los paquetes por un router comprometido</p> <p>Protección: Filtrado de paquetes</p>
---	--

Analista de Seguridad Informática

Capítulo 1. Conceptos básicos



Capítulo 1. Conceptos básicos

Contenido	Ataques
Presentación	
Definiciones	
Tipos de ataques	
	Reenvío
	Una vez capturado un paquete, el atacante puede causar un daño si envía posteriormente el mismo paquete capturado al receptor.
	Existen dos tipos de reenvío: <ul style="list-style-type: none">• Los que identifican partes de información (p.e. password)• Los que simplemente envían un paquete compelto
	<i>El reenvío no funciona con paquetes TCP ya que usan un número de secuencia, a no ser que la secuencia sea fácilmente predecible</i>
	Protección: Rechazar paquetes duplicados, por ejemplo usando marcas de tiempo o números de secuencia

Analista de Seguridad Informática

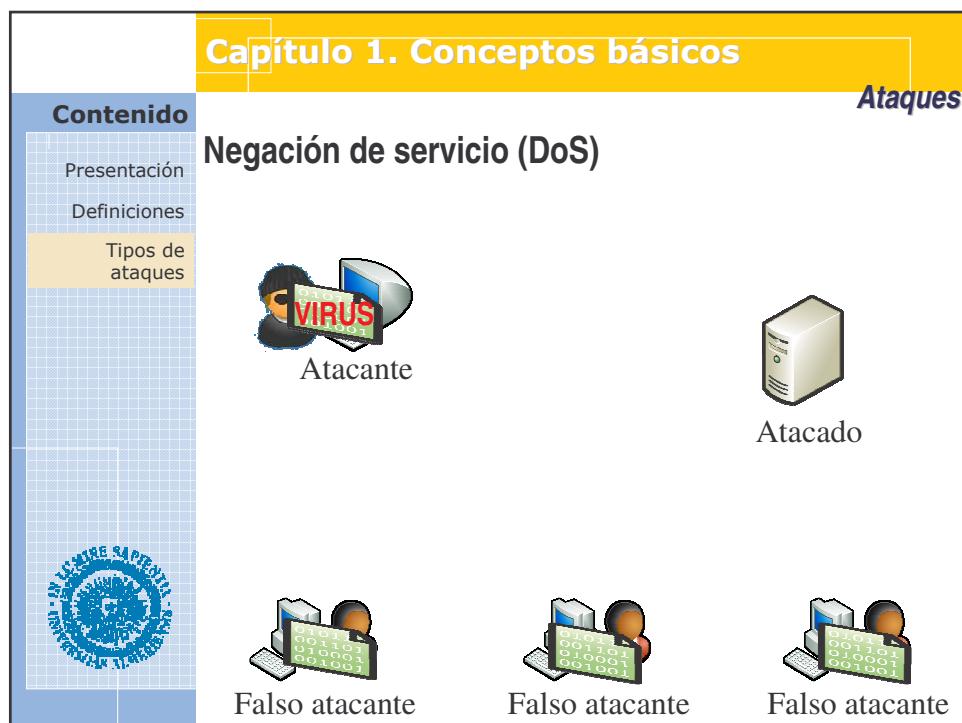
Capítulo 1. Conceptos básicos

Capítulo 1. Conceptos básicos	
Contenido Presentación Definiciones Tipos de ataques	<p>Hijacking</p> <p>Permite a un atacante robar una conexión de un usuario que ya ha sido autenticado.</p> <p>Fallo de conexión</p> <p>User legítimo</p> <p>Servidor</p> <p>Atacante</p> <p>Login: pepe Contraseña: hola00</p>

Capítulo 1. Conceptos básicos	
Contenido Presentación Definiciones Tipos de ataques	<p>Explotar bugs del software</p> <p>Aprovechar errores en la implementación del software para acceder a recursos sin autorización. P.e. comandos inválidos</p> <p>Protección: Actualización del software</p>

Analista de Seguridad Informática

Capítulo 1. Conceptos básicos



PAÍS.com | Un ataque de denegación de servicio colapsa Telefónica.net y Terra.es - TECNOLOGÍA - MÓVIL Y FONOS

Editor Ver Historial Marcadores Herramientas Ayuda

http://www.elpais.com/articulo/internet/ataque/denegacion/servicio/collapse/Telefonica.net/Terra.elpep

gle - ataque "denegación de servicio" Buscar Corrección ortográfica Suscribirse Opciones ataque denegación de servicio

Sábado, 27/1/2007, 19:11:11

PAÍS.com | Tecnología

Ciberpais | Meristation

PAÍS.com > Tecnología

Jn ataque de denegación de servicio colapsa Telefonica.net y Terra.es

Numerosos usuarios no pudieron utilizar su correo electrónico

PAÍS.es - Madrid - 03/03/2006

5 Resultado 0 votos

Los portales Telefonica . Net y Terra.es sufrieron antes de ayer a las nueve de la noche, según fuentes de la compañía Telefónica, un ataque denominado DDoS (Denegación de Servicio) que consiste en lanzar miles de solicitudes de información intentos de visitas por ejemplo) a los servidores de una página web.

La Asociación de Internautas denuncia a Jazztel

a noticia en otros webs

webs en español en otros idiomas

Los portales estuvieron "caídos algún tiempo por la tarde", según las mismas fuentes, que han manifestado que el servicio está restablecido y que "de momento" no saben desde dónde se realizó el ataque.

Pese a que Telefónica ha asegurado que el ataque se produjo antes de ayer, numerosos usuarios siguen manifestando que en los dos últimos días no

publicidad

internet ONO

"Máxima Satisfacción de Clientes como Proveedor de Servicios de Internet de Banda Ancha"



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Estimado usuario,

Hemos detectado algunos ataques desde su cuenta de correo, por lo que su ordenador debe tener algún virus. Para limpiar su ordenador de virus siga las instrucciones **del fichero adjunto**

Nuestros mejores deseos,

El equipo dominio <http://www.dominio.com>

Capítulo 1. Conceptos básicos

Contenido

Presentación

Definiciones

Tipos de ataques

Ataques

Ingeniería social

Aprovechar la buena voluntad de los usuarios para tomar sus privilegios o para dañar su equipo.

Protección: Autentificación e información



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Capítulo 1. Conceptos básicos

Ataques

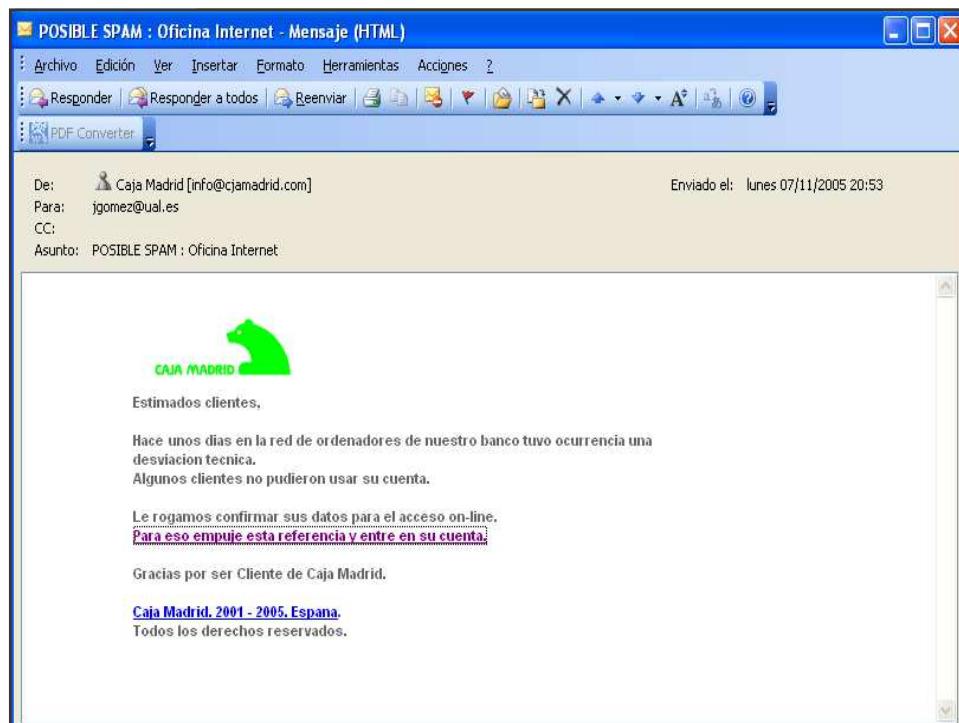
Contenido

- Presentación
- Definiciones
- Tipos de ataques

Phising

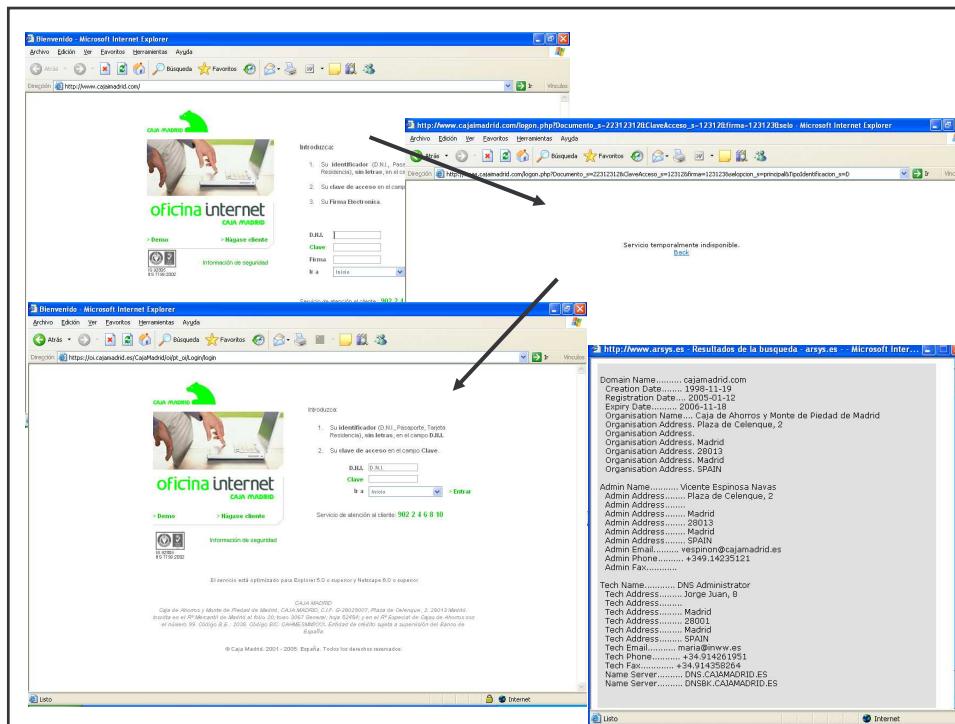
Es una variable de la ingeniería social. A través de mensajes de texto “falsificados” y sitios Web fraudulentos engañan a los usuarios con el fin de que revelen datos financieros, datos personales, contraseñas, etc.

Protección: Firma digital, encriptación e información



Analista de Seguridad Informática

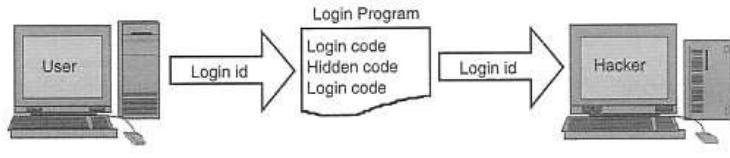
Capítulo 1. Conceptos básicos



Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

Contenido Presentación Definiciones Tipos de ataques 	<h3>Capítulo 1. Conceptos básicos</h3> <h4>Ataques</h4> <h3>Confianza transitiva</h3> <p>Aprovechar la confianza UNIX entre usuarios o hosts para tomar sus privilegios:</p> <ul style="list-style-type: none">•Usuarios: mediante .rhosts•Host: mediante .equiv <p>Protección: Autentificación y filtrado de paquetes</p>
--	--

Contenido Presentación Definiciones Tipos de ataques 	<h3>Capítulo 1. Conceptos básicos</h3> <h4>Ataques</h4> <h3>Ataques dirigidos por datos</h3> <p>Ataque dirigido originado por:</p> <ul style="list-style-type: none">•Virus•Gusanos•JavaScript•Caballos de troya  <p>Protección: Antivirus, firma digital e información</p>
--	---

Analista de Seguridad Informática

Capítulo 1. Conceptos básicos

The screenshot shows a Microsoft Internet Explorer window displaying the 'Alerta-Antivirus' website. The page title is 'Alerta-Antivirus: Buscar Virus y Bulos - Microsoft Internet Explorer'. The main content area is titled 'Encontrados 281 Virus' and lists various viruses with columns for Nombre y Alias, Peligrosidad, Tipo, and Fecha descubrimiento. The viruses listed include Protoride.NAH, Botitos, Sdbot.AH, Protoride.NAG, SdBot.COT, SdBot.COУ, Orpheus, and Zafi.C. The 'Peligrosidad' column uses a green color scale from 1 (Mínima) to 2 (Baja). The 'Tipo' column is mostly red, indicating they are viruses.

Nombre y Alias	Peligrosidad	Tipo	Fecha descubrimiento
Protoride.NAH, Win32/Protoride.NAH [Enciclopedia Virus], W32/Protoride-NAH [Sophos]	2 - Baja		26/11/2004
Botitos, BKDR_BOTITOS.A [Trend Micro], Win32/Botitos.A [Enciclopedia Virus]	2 - Baja		25/11/2004
Sdbot.AH, Backdoor.Sdbot.AH [Symantec]	2 - Baja		24/11/2004
Protoride.NAG, Win32/Protoride.NAG [ESET (NOD32)], W32/Protoride-W [Sophos]	2 - Baja		17/11/2004
SdBot.COT, IRC/SdBot.COT [ESET (NOD32)]	2 - Baja		16/11/2004
SdBot.COУ, IRC/SdBot.COУ [ESET (NOD32)]	2 - Baja		15/11/2004
Orpheus, W32.Orpheus.A [Symantec]	2 - Baja		09/11/2004
Zafi.C, W32/Zafi.C@MM [McAfee], W32/Zafi.C.worm [Panda Software], W32/Zafi.C@mm [ParAvitivirus], Win32/Zafi.C [Enciclopedia Virus], W32.Erkez.C@mm [Symantec]	1 - Mínima		28/10/2004

The diagram is a conceptual model divided into three main sections: 'Contenido' (Content), 'Capítulo 1. Conceptos básicos' (Chapter 1. Basic Concepts), and 'Ataques' (Attacks). The 'Contenido' section includes 'Presentación', 'Definiciones', and 'Tipos de ataques'. The 'Capítulo 1. Conceptos básicos' section contains three entries: 'Adivinación de password' (Password Guessing), 'Tempest' (Tempest), and 'Rubber-Hose' (Rubber-Hose). Each entry has associated text and a 'Protección:' (Protection) box. The 'Adivinación de password' entry describes it as a systematic password cracking method. The 'Tempest' entry describes it as electron emission monitoring. The 'Rubber-Hose' entry describes it as torture for information extraction. The 'Protección:' boxes for each entry provide specific measures: 'Adivinación de password' suggests changing passwords and using digital signatures; 'Tempest' suggests lead and concrete walls; and 'Rubber-Hose' suggests personal defense.

Contenido	Capítulo 1. Conceptos básicos	Ataques
Presentación	Adivinación de password	Prueba sistemática de password de un usuario
Definiciones		Protección: Información (cambiar password) y firma digital
Tipos de ataques	Tempest	Barido de emisión de electrones de los CRTs para observar la información en pantalla de un usuario.
	Rubber-Hose	Protección: Paredes de plomo y hormigón

