Informe de incidentes de seguridad año 2005

cert@rediris.es

30 de enero de 2006

Índice

1. Introducción

El objetivo del presente informe es el de dar un repaso detallado a los problemas más importantes de seguridad detectados en la Red Académica durante el año 2005.

Se muestran aquí no sólo algunos números y estadísticas, sino también una descripción de aquellos problemas más comunes, así como enlaces a sitios que aporten más información y mecanismos para eliminar dichos problemas.

El presente documento, se publica en la Web de IRIS-CERT bajo http://www.rediris.es/cert/doc y junto a los informes de años posteriores. Además, se presenta en la lista de coordinación de seguridad de RedIRIS, IRIS-CERT.

Recomendamos echar un vistazo al informe de operación presentado por IRIS-CERT en las pasadas Jornadas Técnicas de RedIRIS, celebradas en Logroño en Octubre de 2005, disponible aquí. En él, se incluye además información sobre otras actividades y foros en las que participa el equipo de seguridad, así como enlaces a otras presentaciones de interés general.

Por favor, estamos abiertos a cualquier sugerencia por vuestra parte que nos permita mejorar la calidad del presente informe. Por eso, si tienes algo que decirnos, mandamos un correo.

Por último, deseamos agradecer la colaboración de Jesús Sanz de las Heras y Jose Manuel Macías para la elaboración de algunas secciones de este informe.

2. Estadísticas

En estas estadísticas solamente aparecen aquellos problemas de seguridad de los que hemos tenido noticia directa. La clasificación que hacemos según el tipo de incidente, se realiza según la información que nos hacéis llegar, por lo que su exactitud depende en gran medida de la retroalimentación que recibimos de vosotros y de cómo de exactos sois a la hora de describir el problema sufrido y las medidas adoptadas.

Desde aquí instamos a todos los encargados de seguridad de las instituciones afiliadas a que, una vez analizado el problema, nos envíen un correo (manteniendo siempre el código de incidente para facilitar su gestión), con una breve descripción de lo encontrado en la máquina y de la causa real del incidente (gusano, compromiso de root, virus, etc...). Ésto nos permitirá, no sólo proporcionar unas estadísticas más en consonancia con la realidad, sino tener una visión mucho más amplia de lo que está pasando en nuestra comunidad.

El año 2005 arroja las siguientes cifras:

- El número de Incidentes atendidos por IRIS-CERT durante el año 2005 ha sido de 1747, de los que:
  - 346 corresponden a incidentes relacionados con Infracción de copyright [1].
  - 49 de esos 1747 incidentes han sido dirigidos al buzón de consultas o *helpdesk* de IRIS-CERT.
  - También hemos recibido correos en los que aparecía la dirección de IRIS-CERT como Copia (Cc:), bien desde dentro de nuestra comunidad o desde grupos de seguridad internacionales. En total 57 incidentes, la mayoría de ellos referentes a máquinas de otros proveedores de Internet Españoles, y por tanto fuera de la comunidad IRIS.
  - Por último, 47 incidentes han sido Informativos [2].

[1] esta cifra corresponde al periodo comprendido entre Enero a Mayo de 2005, puesto que en la reunión del Grupo de Trabajo de IRIS-CERT celebrado en Málaga en Mayo de 2005 se acordó por consenso que IRIS-CERT no iba a atender más casos relacionados con este tipo de problemas.

[2] Que se refieren a IPs que no están dentro de nuestro ámbito de actuación o casos en los que no se requiere ningún tipo de interacción por nuestra parte.

Para realizar una comparativa con el año anterior, y quitando el número de incidentes referidos a los tipos anteriores, podríamos decir que el número de incidentes reales.ªtendidos durante este año (sin contar copyright, consultas, copia e informativos) sería de 1248, lo que supondría un decremento del 27.18 % con respecto al año pasado en el que se atendieron 1714 incidentes. Este decremento creemos se puede deber al cambio que realizamos el Marzo del año pasado de nuestra herramienta de gestión de incidencias, y a las diferencias de workflow y de clasificación que ello nos ha supuesto, ya que como veremos más adelante, el año 2005 ha sido muy parecido al 2004 en cuanto a tendencias y volumen de incidentes.

En el siguiente gráfico se muestra la evolución de los incidentes de seguridad desde el año 1999.

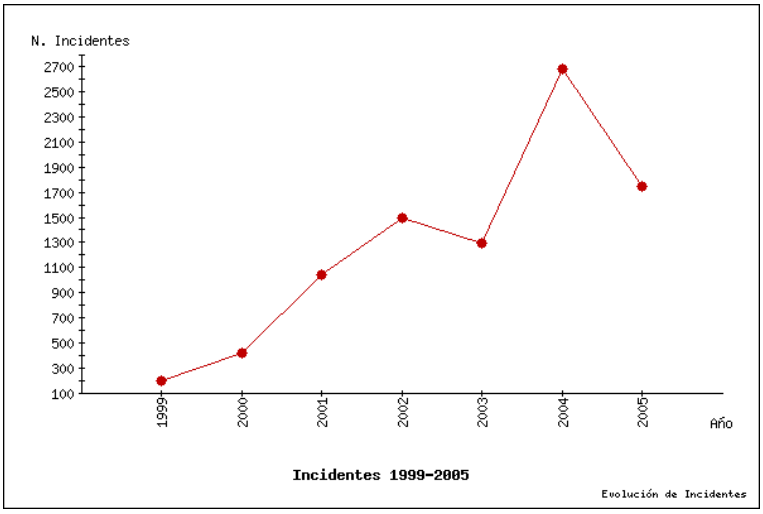

Figura 1: Evolución de incidentes por años

Las cifras detalladas son los siguientes:

Año	**Incidentes totales**	**Incremento**
1999	195	-
2000	416	113.333 %
2001	1038	149.51 %
2002	1495	44.02 %
2003	1294	-13.44 %
2004	1714	32.45 %
2005	1248	-27.18 %

Como mostramos en la figura siguiente, la mayoría de los incidentes que atendemos, como es lógico, se refieren a problemas originados en nuestra comunidad (en total un 93 %), seguidos en un 6 % por aquellos originados en máquinas del dominio .es, a los que IRIS-CERT aún presta un soporte de coordinación de incidentes, y por último un 1 % originados internacionalmente.

2.1. Evolución de los incidentes

En general, como hemos comentado en la sección anterior, 2005 ha sido un año muy parecido al año anterior. Gusano, virus, redes de bots, ataques de fuerza bruta (ssh fundamentalmente), escaneos a puertos con vulnerabilidades conocidas, ataques a servidores Web, DoS, etc.. han sido de los tipos de ataques más vistos durante el año.

De todos ellos, el más persistente a lo largo de todo el año han sido los ataques de fuerza bruta SSH aprovechando contraseñas débiles. Desde que en Agosto del año pasado pareciera una herramienta que permitía realizar este tipo de ataques de forma automatizada, no hemos dejado de recibir quejas de escaneos e intentos de este tipo. En general, estos ataques se basan en acceder al sistema utilizando una cuenta SSH con password débil (y normalmente sin privilegios). Una vez en el sistema, el atacante emplea un exploit del núcleo de Linux en local para conseguir acceso como root, lo que lei permite instalar diversos rootkit y controlar la máquina a su antojo.

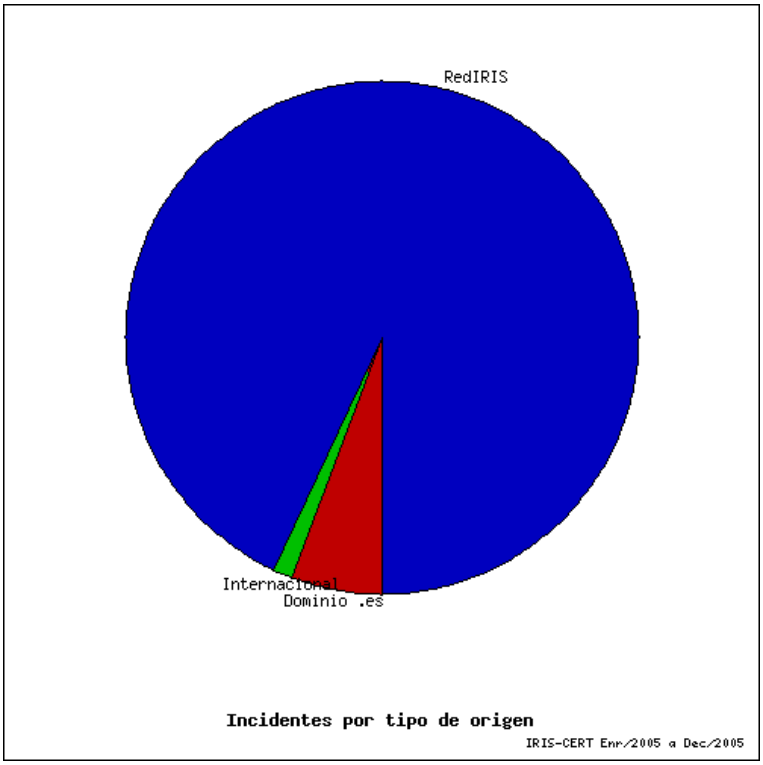

Figura 2: Clasificación según origen de la incidencia

Tras los ataques de fuerza bruta SSH, en el ranking le siguen gusanos y virus (muchos viejos conocidos, apareciendo gran cantidad de nuevas variantes de algunos de ellos como el Beagle, Mydoom o el Sober por citar algunos, y algunos nuevos como el Zotob, Mytob, etc..), seguidos por las las redes de bots o máquinas zombies. Estas redes se suelen utilizar para el envío de correo basura (SPAM), lanzar ataques de DDoS o gestionar servicios de phishing entre otras muchas cosas.

Algunas fuentes destacan que durante el año 2005 el número de vulnerabilidades aparecidas en productos ha aumentado considerablemente con respecto a los años anteriores. SANS Institute publicó a finales de año, una interesante página con las 20 vulnerabilidades más críticas del año, tanto genéricas como por Sistema Operativo.

Por otro lado, el phishing y en general el acceso a servicios de comercio electrónico para la obtención de información de usuarios, ha sido

un problema que se ha ido intensificando durante 2005, no especialmente en la red académica, pero si de forma generalizada en Internet. Lo que al principio de año eran ataques esporádicos, se ha convertido en una verdadera plaga. Existen herramientas que permiten paliar los ataques de este tipo, una de ellas es la utilidad anti-phishing de Netcraft. Además, las últimas versiones de algunos clientes de correo, como Thunderbird también previenen de este tipo de ataques.

Lo mismos ha ocurrido con el SPAM, cuyo crecimiento exponencial está muy ligado a la distribución de virus que incorporar su propio motor SMTP.

El año lo cerramos como se cerró el año 2004. Si a finales del 2004 aparecía un gusano que que utilizaba el popular buscador Google para infectar servidores Web que utilizaban una versión vulnerable de phpBB, modificando sus páginas Web. A finales del 2005 hemos detectado un incremento de los ataques que ejecutan inyección de código contra sitios web que tienen implementados módulos vulnerables tales como el awstats [3].

Si hablamos de cierres, a finales de Diciembre y en plenas vacaciones de Navidad, se conocía un grave fallo en la forma en la que Windows maneja los archivos Windows Media File (.WMF), que afectaba a todas las versiones de Windows. La forma de explotar este fallo, tan sólo visualizando una imagen, y la controvertida respuesta de Microsoft en cuanto a la distribución del parche correspondiente, ha generado un gran revuelo y expectación en el mundillo, obligando a Microsoft a romper su ciclo de actualizaciones mensuales.

Por último, se confirma la tendencia de los últimos años con respecto a la modificación del tipo de objetivo. Los más afectados son las máquinas de usuarios finales, conectados permanentemente y poco protegidos. Esto hace que el número de ordenadores asaltados sea mayor y los ataques realizados con ellos, más masivos. Algunas razones que explicarían este cambio podrían ser:

- Aumento del ancho de banda y prestaciones de los equipos conectados permanentemente

[3] Más información sobre vulnerabilidades relacionadas con la Web más adelante en este documento

- Baja protección de los equipos
- Imposibilidad de grandes proveedores de realizar acciones preventivas
- Uso de redes móviles

La siguiente gráfica muestra la distribución de incidentes atendidos por el equipo en los distintos meses del 2005.

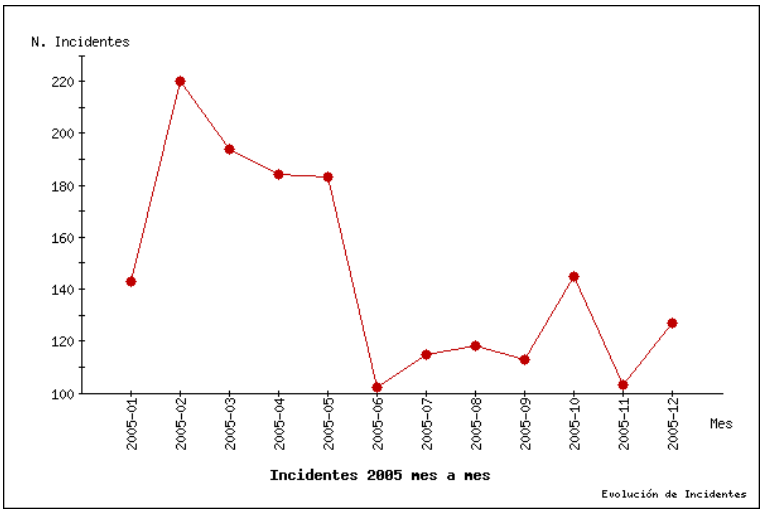

Figura 3: Evolución de incidentes por meses

Los datos detallados son los siguientes:

Fecha	Total
2005/01	143
2005/02	220
2005/03	194
2005/04	184
2005/05	183
2005/06	102
2005/07	115
2005/08	118
2005/09	113
2005/10	145
2005/11	103
2005/12	127

Para finalizar, y completar lo descrito con anterioridad, os mostramos la siguiente gráfica con una distribución de incidentes según nuestra taxonomía de alto nivel.

Como veis, existe un aplastante dominio de los ataques debidos a escaneos. Estamos convencidos que detrás de la mayoría de ellos se encuentra un problema mayor y por tanto la causa real del escaneo, por lo que os pedimos que si queréis que la información que os presentemos sea lo más veraz posible, nos contéis lo que realmente ha ocurrido o habéis encontrado, y no tan sólo contestéis con un simple *"Problema resuelto"* ;-).

2.2. Incidentes de SPAM 2005

La posibilidad de llevar a cabo fraudes con suculentos beneficios económicos ha despertado el interés de spammers y hackers para participar en un negocio controlado por las cibermafias internacionales. La distribución de virus para controlar PCs, el alquiler de granjas de PC zombies para distribuir spam, troyanos o phishing, ha sido un verdadero mercado negro y atractivo negocio que está provocando un crecimiento

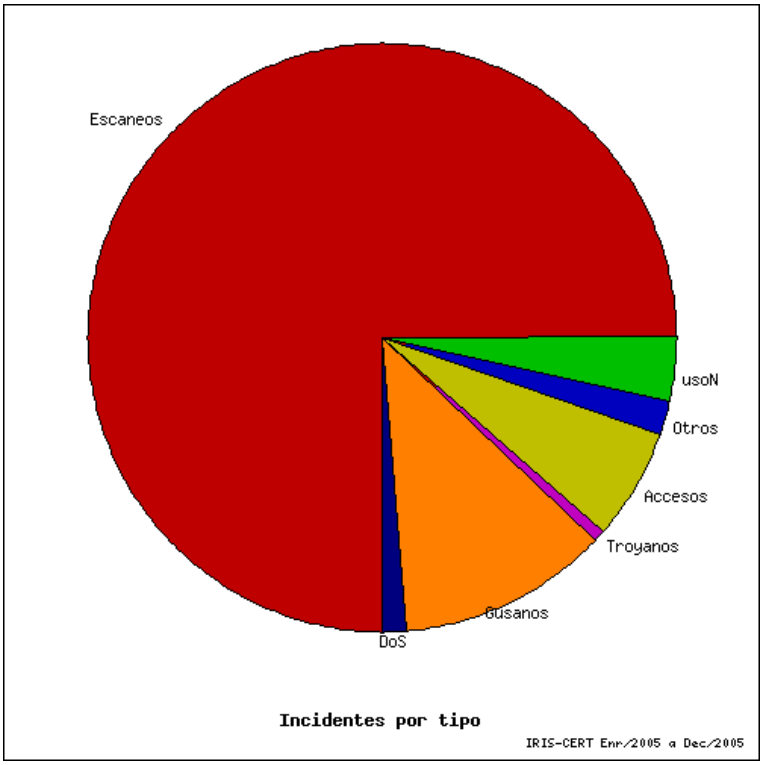

Figura 4: Incidentes por tipo según taxonomía

desmesurado del spam y por supuesto un aumento de la inseguridad en el Red.

El aumento exponencial de tráfico basura (spam) está provocado casi exclusivamente por malware (troyanos, spyware, ..) instalados en PCs con conexión residencial (ADSL, cable). Estos virus incluyen capacidades de motor SMTP lo que les permite actuar como un servidor de correo autónomo, y controlar todo el proceso de envío y distribución de correo sin necesidad de pasar por el operador del usuario.

Según las estadísticas de la red de sensores del Centro de Alerta Antivirus, en el último año el 85 % de los correos analizados corresponden a virus con estas capacidades. Estos virus comprometen miles de máquinas (zombies) que son gestionadas como una red (botnet) para diferentes actividades maliciosas: phishing, spam comercial, difundir virus etc. Las máquinas infectadas pertenecen en su gran mayoría a

redes de acceso residencial (cable, ADSL etc.). Spamhaus.org tiene una lista de 4 millones de máquinas infectadas, unas 60-100 mil máquinas por semana. Para propagarse, los virus analizan el disco del ordenador comprometido buscando direcciones de correo en libreta, ficheros etc. Una vez con direcciones de correo de destino ya puede llevar a cabo la distribución de miles de mensajes. En el proceso de envío, el virus falsifica la dirección del emisor, ésta es una de las tácticas más habituales de los virus y su solución uno de los frentes más activos en la lucha contra el spam.

2.3. Vulnerabilidades relacionadas con la Web

2.3.1. XSS

Durante 2005 han sido descubiertas numerosas vulnerabilidades *Cross Site Scripting* en sus distintos tipos. Mencionamos sólo algunas de las aplicaciones afectadas, que por su gran difusión pueden afectar a más usuarios:

1. ASP.Net
2. PhpNuke
3. phpBB
4. Oracle XMLDB
5. phpmyadmin/phpldapadmin/phppgadmin
6. Mambo

Estas vulnerabilidades se han intentado aprovechar en ocasiones mediante el rastreo por "fuerza bruta"de servidores web que pudieran contener las aplicaciones afectadas.

Como siempre, os recomendamos actualizar a la última versión de estas aplicaciones.

2.3.2. SQL Injection

Las vulnerabilidades que permiten inyección de código SQL en distintas aplicaciones también han sido numerosas y constituyen una de las

formas más utilizadas de ataque. Mencionamos también algunas de las aplicaciones que se han visto afectadas por ataques de este tipo:

1. ASPnuke
2. PhpNuke
3. Gallery
4. phpBB
5. phpmyadmin
6. Mambo

2.3.3. Vulnerabilidades en servidores web

La rama 1.3 de apache no ha tenido serias vulnerabilidades, mientras que la 2.0 sí que se ha visto afectada por varios fallos que han sido corregidos corregidos en distintas revisiones.

De la rama 1.3, la última versión disponible es la 1.3.34, que corrije:

1. *SECURITY: core: If a request contains both Transfer-Encoding and Content-Length headers, remove the Content-Length, mitigating some HTTP Request Splitting/Spoofing attacks. This has no impact on* $mod_proxy_http, yetaffectsan$
   $E : chunkedovertheContent-Lengthpurportedvalue.[PaulQuerna, JoeOrton]$

   De la 2.0, la última versión es la 2.0.55, que solventa :

   1. *SECURITY: CAN-2005-2700 (cve.mitre.org)* $mod_ssl : Fixasecurityissuewhere"SSLVe$
      $locationcontextif"SSLVerifyClientoptional"wasconfiguredinthevhostconfiguration$
   2. *SECURITY: CAN-2005-2088 (cve.mitre.org) proxy: Correctly handle the Transfer-Encoding and Content-Length headers. Discard the request Content-Length whenever T-E: chunked is used, always passing one of either C-L or T-E: chunked whenever the request includes a request body. Resolves an entire class of proxy HTTP Request Splitting/Spoofing attacks. [William Rowe]*
   3. *SECURITY: CAN-2005-2728 (cve.mitre.org) Fix cases where the byterange filter would buffer responses into memory. PR 29962. [Joe Orton]*

4. *SECURITY: CAN-2005-2088 (cve.mitre.org) core: If a request contains both Transfer-Encoding and Content-Length headers, remove the Content-Length, mitigating some HTTP Request Splitting/Spoofing attacks. [Paul Querna, Joe Orton]*

5. *SECURITY: CAN-2005-1268 (cve.mitre.org) $mod_ssl : Fixoff - by - oneoverflowwhilstprintingCRLinformationat"LogLeveldebug"whichcouldbetriggeredifcomsterncsc.com >]$*

   La rama 2.2, a pesar de ser más reciente [4], también contiene fallos críticos:

   1. *SECURITY: CVE-2005-2970 (cve.mitre.org) worker MPM: Fix a memory leak which can occur after an aborted connection in some limited circumstances. [Greg Ames]*

2. *SECURITY: CVE-2005-2700 (cve.mitre.org) $mod_ssl : Fixasecurityissuewhere"SSLVerifylocationcontextif"SSLVerifyClientoptional"wasconfiguredinthevhostconfiguration.[Joe$*

   Recomendamos la revisión de fallos de las últimas versiones, disponibles en las siguientes URls para las distintas ramas:

   1. Vulnerabilidades rama 1.3.x de apache
   2. Vulnerabilidades rama 2.0.x de apache
   3. Vulnerabilidades ramas 2.1.x y 2.2.0 de apache

   Se han encontrado también fallos relacionados con PHP en las ramas 4.x y 5.x, recomendamos comprobar en el changelog de las últimas versiones si pueden afectar (rama 4.x de PHP, y rama 5.x de PHP)

2.3.4. Acceso a webcams

Muchas cámaras IP que incluyen un servidor web para visualizar imágenes, y se ha comprobado que en buena parte estas cámaras se encuentran totalmente accesibles desde Internet.

En la parte del cliente, tanto Internet Explorer, como Mozilla y navegadores basados en Mozilla se han visto afectados por distintos fallos de seguridad. Recomendamos actualizar a la versión más actual de estos navegadores.

[4] Es la que hasta hace poco era rama de desarrollo 2.1.x

2.3.5. Phishing

La web fue siguió siendo utilizada y vio incrementado el número de estafas "phishing", especialmente las relacionadas con la suplantación de sitios web de entidades bancarias. Existen herramientas que permiten paliar los ataques de este tipo, una de ellas es la utilidad anti-phishing de Netcraft [7].

3. Links de interés

A continuación podéis encontrar algunos enlaces a documentos donde se describen algunos de los problemas más significativos detectados durante el año 2005.

1. Gusanos
   - *a*) Beagle.CL
     - http://alerta-antivirus.red.es/virus/detalle$_v$*irus.html*?*cod* = 5424
   - *b*) Bagle.BV
     - http://alerta-antivirus.red.es/virus/detalle$_v$*irus.html*?*cod* = 5259
   - *c*) Beagle.BQ
     - http://alerta-antivirus.red.es/virus/detalle$_v$*irus.html*?*cod* = 4990
   - *d*) Beagle.AY
     - http://alerta-antivirus.red.es/virus/detalle$_v$*irus.html*?*cod* = 4683
   - *e*) Slammer
     - http://securityresponse.symantec.com/avcenter/venc/data/w32.sqlexp.worm.ht
   - *f*) Linux/Lupper.worm.b
     - http://vil.nai.com/vil/content/v$_1$36856.*htm*
   - *g*) Mytob
     - http://alerta-antivirus.red.es/virus/busca$_v$*irus.html*?*pclave* = *Mytobbuscar* = *Buscar*

h) Zotob
   - http://alerta-antivirus.red.es/virus/busca$_v irus.html?pclave = Zotobbuscar = Buscar$

i) Mydoom
   - http://alerta-antivirus.red.es/virus/busca$_v irus.html?pclave = mydoombuscar = Buscar$

j) Sober
   - http://alerta-antivirus.red.es/virus/busca$_v irus.html?pclave = mydoombuscar = Buscar$

k) SDBot
   - http://alerta-antivirus.red.es/virus/busca$_v irus.html?pclave = SDBotbuscar = Buscar$

2. Troyanos
   a) Troj/Winser-A
      - http://www.unixwiz.net/research/winser-a.html
3. Bots
   a) IRCBot.KN
      - http://antivirus.hispavista.com/virus$_8 6545_i rcbot - kn$
4. Vulnerabilidades
   a) Vulnerabilidad en el tratamiento de ficheros WMF de Microsoft
      - http://www.microsoft.com/technet/security/advisory/912840.mspx
5. Otros
   a) Ataques de fuerza bruta SSH
      - http://www.whitedust.net/article/27/Recent%20SSH%20Brute-Force%20Attacks/
   b) SANS Top 20
      - http://www.sans.org/top20/
   c) Grupo de Trabajo de IRIS-CERT. Logroño. Octubre 2005
      - http://www.rediris.es/cert/doc/reuniones/cord/jt2005/