

<u>0.</u> CONTENIDOS
----------------------

<u>0.</u> (saq_con.txt)	Contenidos	Dark Raver
<u>1.</u> (pres.txt)	Presentacion	El Siciliano
<u>2.</u> (aniv.txt)	Primer aniversario	El Nuevo Eljaker
<u>3.</u> (num.txt)	Numeros especiales	Villalonga
<u>4.</u> (iberpac.txt)	Introducion a Iberpac	El Nuevo Eljaker
<u>5.</u> (codigo.txt)	Codigo Penal	Recopilacion/Dark Raver
<u>6.</u> (puertos.txt)	Puertos	Valfadir
<u>7.</u> (cb.txt)	Codigos de barras	Warezzman
<u>8.</u> (scan.txt)	Wardialing	Warezzman
<u>9.</u> (report.txt)	Conclusiones de la UC97	Organizadores

Hola amigos, soy Dark Raver y soy el encargado de cordinar esta edicion especial de la saqueadores. Este numero esta hecho especialmente para la UnderCon '97 que a pesar de sus muchos problemas de organizacion parece que al final se va a celebrar.

Como veis el numero de articulos no es demasiado elevado... parece que hay una plaga de impuntualidad y de incumplimientos de promesas, asi que unos cuantos articulos que me habian prometido no han llegado... Aun asi creo que el nivel esta bastante bien.

Pero bueno, no me voy a enrollar mas porque de la presentacion ya se encarga nuestro amigo el Siciliano.

Grupo Saqueadores

"Seguro que vais a ser capaces de organizar un congreso de hackers en 3 meses?"

EL DUKE DE SICILIA

\*EOF\*

Bienvenidos al oscuro mundo del underground murciano.

Como parte de las celebraciones por el primer aniversario de la Saqueadores se va a celebrar un pequeño congreso underground en la ciudad de nacimiento de nuestra publicación.

El congreso se llamara UnderCon '97 y despues de muchos problemas al final la cosa se va a celebrar. Espero que esteis entre los afortunados visitantes.

Para el resto de los componentes del underground aqui teneis estos textos y dentro de poco sacaremos el segundo numero especial de la saqueadores, la edicion just-in-time de la UnderCon, realizada en directo por los asistentes, con comentarios sobre lo acontecido, resúmenes de las mesas redondas y artículos colectivos. Todo escrito por los asistentes a la con.

Los textos de este numero han sido escritos la mayoría (Excepto de de valfadir) por componentes de la escena underground murciana que son los que estan montando todo este tinglado y los que estan demostrando que el hacking tambien es posible lejos de las grandes urbes.

No son unos buenos organizadores pero sin duda son unos hackers/phreakers cojonudos.

Os dejo con su trabajo.

El Duke de Sicilia  
el\_duke@usa.net

"You have nothing left but destruction"

WASTING PROGRAM

\*EOF\*

Feliz aniversario:

Un poco de historia...

A finales del mes de agosto del año 1996 aparecio un extraño mensaje en el area de hacking de BBS Club, tenia un logo formado por caracteres ascii y estaba realizado por alguien apodado Eljaker. Pretendia ser una especie de publicacion basada en temas del underground informatico.

La historia comenzo unos meses antes, cuando un pequeño grupo de avezados informaticos habia elegido este area de mensajería como lugar de reunion. El nivel era bastante bajo, pero ya empezaban a despuntar algunas habilidades destacables. El grupo estaba desorganizado y muchos de sus componentes preguntaban dudas que en ningun sitio encontraban respuesta.

Por eso algunos de los mas veteranos en estos temas deciden fundar el grupo Saqueadores cuyo principal fin era distribuir entre los que deseaban aprender la informacion que pedian.

Los tres miembros fundadores de este grupo fueron Warezzman, Dark Raver y como no, yo, Eljaker. Por aquel entonces eramos un grupillo de hackers novatos y con pocos conocimientos, pero con muchas ganas... y a la larga hemos demostrado que podiamos aprender muy rapido.

Asi finalmente ademas de la activa conversacion en el area y el intercambio de informacion entre los componentes del grupo, se crean varias paginas webs y se decide sacar a la calle una publicacion.

Los dos primeros numeros fueron una especie de ensayo, en teoria no tenian que haber salido de BBS Club, pero Warezzman decidio ponerlos en su pionera pagina del hacking hispano "Iberhack" y aqui empezo la carrera.

A partir de entonces la evolucion fue meteorica, se fueron añadiendo mas y mejores articulistas y la calidad de la publicacion como podreis apreciar se ha elevado hasta niveles inimaginables hace un año.

La evolucion ha sido algo movida, con varios cambios de editor y con algunas movidas serias, pero parece que la cosa sigue. (A menos que Telefonica encuentre a Paseante tras su artículo sobre Infovia :-)

Y es que hay que tener en cuenta que en aquellos lejanos tiempos todavia no habia ninguna publicacion sobre hacking en España. Apenas habia media docena de paginas webs dedicadas al tema, y los textos se podian enumerar casi de memoria.

Ni mencionar que apenas habia grupos organizados y que aparte de unas pocas BBS no habia medios de comunicacion estables entre los componentes de la scene.

Hoy en dia...

Actualmente solo teneis que poner en cualquier buscador en castellano la palabra "hack" para daros cuenta de como ha cambiado la cosa. Todo esto se ha construido en apenas un año y si sigue asi puede alcanzar niveles internacionales.

Internet ha sido sin duda el canal vitalizador del movimiento y el principal punto de contacto de los antes aislados hackers hispanos.

Pero no todo ha sido positivo en esta rapida evolucion, internet ha entrado

demasiado fuerte y algunos han caído. Por ejemplo las míticas BBS como BBS Club han tenido que cerrar y los veteranos hackers se han visto abrumados por la enorme avalancha de hackers novatos.

Pero los avances han sido mayores que las pérdidas y podemos decir que el panorama hack español goza de buena salud, contando con un buen número de grupos y con un comportamiento bastante ético. (Aunque algunos payasos van por ahí metiéndose con los pocos que hacen algo por mejorar la scene)

Vuelta a la actividad...

Como sabéis estoy algo alejado de la publicación, pero a pesar de mi retirada de la vida pública (no de la activa) me han pedido que escriba un artículo conmemorativo de este primer aniversario.

Y es que este pasado agosto (o para los internautas este septiembre) se celebra la salida a la luz del primer número del magazine "Saqueadores"

Tengo que reconocer que no empezamos con muy buen pie, la publicación pretendía servir de manual de iniciación para los más novatos y sus contenidos y su nivel técnico dejaban bastante que desear.

Ahora, un año después y con un nivel bastante superior al que tenía cuando empecé reconozco que los primeros números son muy pobres. Pero por suerte la vida sigue y uno va aprendiendo más y más.

Espero que la publicación os haya servido para aprender algo nuevo y de paso para pasar un rato divertido. Porque estas son las razones principales de su existencia.

Y ahora con un poco más de experiencia, el nuevo nivel de la publicación nos hará ser realmente buenos hackers.

Correo...

Me están llegando mensajes de conocidos quejándose del nuevo nivel que está alcanzando la revista. Parece que la Saqueadores ha superado el nivel más difícil y ya no es una publicación de iniciación. Me parece muy bien, ya hay otras publicaciones de iniciación, ahora la Saqueadores tiene que enfrentarse al futuro y ocupar el vacío de las publicaciones técnicas en español.

Sin duda los últimos números son los mejores y espero que la cosa siga así. Y si pensáis distinto, a que esperáis para fundar vuestra propia publicación para no iniciados.

Desde aquí quiero mandar una felicitación a Paseante por la nueva saqueadores y espero que siga consiguiendo artículos tan buenos como el de Infovia.

También me han preguntado si voy a volver a escribir algún artículo... la respuesta es que pronto escribiré algo, pero solo en el momento en el que este seguro de que el artículo será tan cojonudamente nuevo que nadie podrá echarme a la cara que hace un año era un completo novato. Por ahora podéis conformaros con un par de artículos que voy a rescatar del baul de los recuerdos.

Despedida...

Solo era eso, os animo a todos a seguir. A los novatos a seguir aprendiendo, y a los veteranos a seguir compartiendo la informacion. Y es que esta es nuestra razon de ser, somos hackers, pero somos algo mas que eso, somos la generacion de la informacion.

'LA INFORMACION ES NUESTRO ARMA CONTRA SUS SECRETOS'  
(La informacion debe ser libre)

El Nuevo Eljaker

\*EOF\*

NNNNNNNNNNNNNNNNNNNNNNNNNNNN  
 N N  
 N NUMEROS ESPECIALES N  
 N N  
 NNNNNNNNNNNNNNNNNNNNNNNNNNNNN

"Give me hardcore!"

[Historia]

Hace unos cuatro meses escaneando en busca de los modems de un conocido hospital de Murcia capital, Villalonga dio con algo raro... un grupo de numeros consecutivos que ofrecian una respuesta bastante extraña.

Al principio penso que era uno de los muchos errores que suelen dar las centrales antiguas, pero tras una serie de pruebas comprobe que esos numeros no eran fallos... estaban hay para alguna extraña meta.

Despues de 4 meses de investigaciones y pruebas infructuosas, Villalonga se rinde y decide sacar a la luz publica este curioso suceso en busca de alguien que consiga sacar algo en claro.

[Resultados]

Los resultados son pocos, despues de varios escaneos de la zona lo unico que se conoce son los sintomas, pero no se ha conseguido ninguna pista fiable de la verdadera naturaleza de estos numeros.

LEYENDA

(c) Comunica

(ne) No existe -> Aparece la tipica voz femenina con la frase "El numero marcado no existe"

(tlargo) Tono largo -> Tono/chirrido largo de unos 3 o 4 segundos (A veces incluso 5 o 6) Parecido al sonido que se oye al descolgar en una cabina.

(tcorto) Tono corto -> Tono/chirrido parecido al anterior pero muy corto de 0.5 a 2 segundos.

(nada) Nada -> Descuelga y no se oye nada, incluso apenas se oye el ruido de la linea.

(voz) Aparece una voz -> Una voz de hombre, no grabada (?)

(lcolapsada) Linea colapsada -> Aparece el mensaje de que la linea esta colapsada en este momento.

"/" -> Numero que varia su respuesta.

360700 - Servicio Pymes de telefonica, activo de 8.30 a 18.30 en dias laborables, el resto del dia aparece una grabacion.

[...]

360750 - (ne)

[...]

360790 - (c)

91 - (c)

92 - (c)

93 - (c)

94 - (c)

95 - (c)

96 - (c)

97 - (c)

98 - (c)

99 - (c)

360800 - (tcorto)

01 - (c)  
02 - (c) / (ne)  
03 - (c)  
04 - (c)  
05 - (c)  
06 - (lcolapsada)  
07 - (tcorto)  
08 - (c)  
09 - (c)  
360810 - (c)  
11 - (c)  
12 - (c)  
13 - (c)  
14 - (c)  
15 - (c)  
16 - (tcorto)  
17 - (c)  
18 - (c)  
19 - (ne) / (c)  
360820 - (nada) / (voz) / (c) / (ne)  
21 - (ne)  
22 - (ne)  
23 - (ne)  
24 - (tlargo)  
25 - (tcorto) / (c)  
26 - (tlargo) / (c)  
27 - (c) / (tcorto)  
28 - (nada)  
29 - (ne)  
360830 - (c) / (ne)  
31 - (ne)  
32 - (ne)  
[...]  
360900 - Hospital Morales Meseguer

#### [Características]

- 1) La mayoría de los números y la mayor parte del tiempo comunican.
- 2) Cuando cogen la línea, lo hacen sin dar tono de llamada. Es decir, se marca y al momento "descuelgan" sin ningún tipo de tono. (Como por ejemplo pasa en el 0XX, lease 055, 048, etc...)
- 3) Los números al descolgar y dar el "chirrido" se quedan en silencio, igual que los números que no dan nada, y no responden a ninguna de las teclas del teclado del teléfono (multifrecuencia) No importa el número de veces que pulses las teclas o el tiempo que permanezcas con la conexión. Hemos estado 5 minutos sin colgar y la conexión no se perdía.
- 4) No son carriers listillo :) lo hemos probado y además son muy cortos. (Por supuesto tampoco son faxes)
- 5) Tiene el precio de una llamada local.
- 6) Algunos números varían su respuesta.
- 7) Descripción de la zona:  
--> 36XXXX, En esta zona están los teléfonos de la mayoría de los centros públicos de Murcia: hospitales, ministerios, universidades, etc...  
--> 360XXX, Abundan los teléfonos de Telefonica: Oficinas, atención a pymes, etc..., uyyy! como suena eso...
- 8) Una pista importante, suelen comunicar más en horarios de oficina.
- 9) Aunque no dan tono de llamada, el retardo entre llamada y respuesta es más larga. Incluso estando en Murcia capital tarda bastantes segundos en dar el mensaje de "El número marcado no existe" por ejemplo.

## [Especulaciones]

En cuatro meses han aparecido montones de teorías pero ninguna comprobada o factible.

a) Son algún tipo de servicio de alarma -> :-? Puede ser... pero? Hay algunos síntomas que no cuadran. No dan tono de marcado, cosa que solo hacen números muy especiales. Algunos varían su respuesta y otros no...

b) Son loops -> Parece lógico, hay números que cumplen las características del número bajo y del alto. Pero después de varias pruebas no hemos tenido éxito. Una de las pistas más intrigantes, es que en uno de los números candidatos a ser un extremo de un loop apareció una voz. Para colmo muy poca gente sabe lo que es un loop y según parece en España nunca se ha encontrado uno.

c) Son PBX -> Pueden ser centralitas privadas, pero es poco probable. No dan tono de llamada (lo cogen al instante) y no responden al envío de tonos.

d) Son cabinas -> Casi seguro que no... Las cabinas sí dan tono de llamada y generalmente nadie descuelga.

--> Aunque queda la probabilidad de que sea el famoso modem de las cabinas que sirve para avisar a la central del estado de la cabina. Según rumores estos modems conectaban con la central a través de iberpac, pero no sería raro que también lo hicieran a través de un número normal.

e) Son números de test de Telefonica -> Es casi seguro, por la zona donde están y por su comportamiento. Pero el problema es averiguar que son y para que son usados.

f) Puede ser algún tipo de servicio del hospital Morales Meseguer... aunque parece poco probable que tengan 30 números ocupados.

## [Conclusiones]

Las conclusiones son estas:

-No tenemos ni pajolera idea de lo que son. Hemos preguntado a varios destacados phreakers y no hemos conseguido ninguna pista concreta.

-Telefonica tiene montones de regalitos ocultos en las líneas esperando a ser descubiertos.

-20 pelas por llamada desde una cabina pueden parecer poco, pero a la larga se acaba gastando una pasta.

Esperamos que con la salida a la luz pública de esta información se consigan nuevos datos y pistas sobre estos números que nos permitan averiguar que son o para que sirven. Si lo averiguamos no dudeis de que lo haremos público.

"968-PHREAK... primer tono... descuelgan... PITA!!! ESTAMOS  
CONECTADOS!!!"

Villalonga

...Ah! se me olvidaba los hospitales de la región de Murcia están comunicados a través de una red de ordenadores y la mayoría tiene un modem conectado al teléfono.

Por si a alguien le interesa el numero del modem del hospital que buscaba Villalonga cuando encontro la zona es este: 360919, que corresponde al Hospital Morales Meseguer, pero esto ya es otra historia... (Para mas informacion os remito al expediente 02)

Villalonga

\*EOF\*

## Introduccion a Iberpac

-----

"...porque no somos uno, somos multitud"

SINIESTRO TOTAL

## Presentacion

=====

Aprovechando mi vuelta a la actividad con el articulo del primer aniversario, he buscado en el baul de los recuerdos y he sacado un pequeño articulo sobre Iberpac que tenia a medio hacer.

Se llama "Introduccion a Iberpac" y es un pequeño manual de iniciacion para los que llegan ahora a la scene. El articulo sirve como recuerdo de los antiguos tiempos en los que Iberpac era el nucleo de la cultura hack en nuestro pais, hasta la llegada de internet.

Esto no quiere decir que lo que aqui se explica no sirve, NO, lo que digo en el articulo es todavia aplicable. Iberpac no esta muerta, sigue existiendo y guarda muchos secretos que habian sido olvidados por la mayoria de los hackers.

Y recuperando el espiritu de las antiguas BBS os traigo informacion libre y gratuita para que la disfruteis.

Aprovechadla

## Que es Iberpac?

=====

Iberpac es una red de datos creada por Telefonica hace unos cuantos años, cuando todavia casi nadie usaba internet.

Es usada principalmente por empresas privadas y entes publicos (Y por la propia Telefonica) Esto hace que la mayoria de los ordenadores de la red sean de acceso privado, cosa que hace muy atractiva la red para posibles intrusos.

A pesar de esto la red esta siendo olvidada por los nuevos hackers que son bastante comodis y se conforman con la facilidad de acceso de internet.

## Glosario de terminos

=====

(\*) En el texto uso principalmente los terminos en ingles, si os interesa en el glosario tambien incluyo su traduccion.

PAD - Packet assembler/disassemble --> EDP - Ensamblador/desensamblador de paquetes = Dispositivo que permite la conexion de terminales (asincronos) a una red de conmutacion de paquetes.

CCITT (ITU-T) = No os pongo lo que significan las siglas :) pero es un organismo internacional encargado de establecer los estandares sobre telecomunicaciones.

NUI - Network User Identifier --> IUR (Identificativo de Usuario de la Red =

Codigo de identificacion de cada usuario. Similar al nombre de cuenta en internet.

CVC - Canales Virtuales Conmutados

NUA - Network User Address --> NRI = Es la direccion de un host. Similar a la ip en internet.

X25 = Estandar de comunicacion entre terminales en modo paquete a traves de redes dde transmision de datos.

PSN - Packet Switched Network --> RCM - Red de conmutacion de paquetes = Red de comunacion mediante circuitos virtuales.

Como funciona?  
=====

El funcionamiento de Iberpac es similar al de cualquier red de ordenadores. Cada sistema conectado tiene un identificativo (NUA) que hay que conocer para conectarse.

Iberpac es una PSN basada en el estandar X25. No voy a explicar todos los detalles de su funcionamiento ya que me ocuparia bastantes articulos, si quereis mas informacion sobre esto os recomiendo que os leais algun libro de telecomunicaciones que hable de Iberpac (Hay varios)

En internet tambien hay algo de informacion sobre el tema.

Para conectarse desde un PC es necesario un programa que emule un tipo de terminal y un PAD al que conectarse. El PAD se encarga de traducir la comunicacion de nuestro terminal en un formato compatible con el estandar de la red, el X25.

En España hay 4 PADs publicos nacionales y un buen numero de privados. Los 4 PADs nacionales son el 041, 042, 047 y 048. Cada uno para un fin diferente.

En esta tabla os dara una idea de su coste y del tipo de terminales que acceden por cada numero.

#-----#-----#-----#-----#-----#	Tipo	Pasos iniciales	Normal	Reducida	Punta	
#-----#-----#-----#-----#-----#						
	X-28 acceso 047	2	21,4	34,2	15,6	
	X-28 acceso 048	2	116,3	154,1	90,5	
	X-32 acceso 041	2	21,4	34,2	15,6	
	X-32 acceso 042	2	116,3	154,1	90,5	
#-----#-----#-----#-----#-----#						

El 047 y el 041 son mas caros porque permiten la llamada a cobro revertido. (En realidad no es cobro revertido :- ) sino que te lo cobran, pero no necesitas un NUI/password para usarlos)

Los programas de comunicacion para ordenadores personales normalmente son de tipo X28 (asincronos)

Como conectarse?  
=====

Hay varias maneras de conectarse a Iberpac, pero la que mas os interesara seguro que es la tercera:

I) Disponiendo de un PAD privado (Perteneiente a algun organismo publico o empresa) y conectando a traves de el mediante un terminal directo o por telefono. Esta solucion puede ser la mas barata, pero necesitareis que vuestra empresa disponga de PAD o tendreis que localizar algun PAD escaneando. (Haciendo wardialing por vuestra zona)

II) Contrantando con telefonica una linea de comunicacion con Iberpac. De esta manera y pagando una modica cantidad os proporcionaran un manual de uso y un identificativo.

Tarifas (Tal vez esten anticuadas)

Suscripcion: Nada  
Configuracion: 1000 Pts  
Mensual: 600 Pts por NUI  
Conexion: 14 Pts por minuto  
Volumen: 10 Pts cada 10 segmentos  
Cargo minimo: 24 Pts por conexion  
Acceso telefonico: Variable

El identificativo esta compuesto de un NUI y de un password. El formato de estos ha cambiado varias veces y si no estoy muy anticuado creo que el NUI era de 9 caracteres y el password de 6.

No se porque esa mania de cambiar tanto de formato, no saben que nosotros no nos rendimos... pueden correr, pero no escapar...

Para conectarse el proceso es muy sencillo, solo hay que seguir las indicaciones que vienen en el manual que entrega Telefonica con el contrato. Si habeis tenido suerte y habeis conseguido un identificativo por otra via menos ortodoxa :-)) aqui teneis un pequeno guion:

1. Coger un programa de comunicaciones/terminal tipo Telix, minicom o el terminal de w95.
2. Seleccionar los parametros de comunicacion a 7E1 y emulacion de terminal tipo VT100.  
Es la emulacion mas usada, aunque tambien se pueden usar otras.  
Normalmente al conectar se os pedira elegir el tipo de terminal usado.
3. Marcar del 048 (ATDT048)
4. Cuando se realice la conexion (CONNECT) teclear dos puntos: '..'
5. Aparecera el prompt: 'IBERPAC<'
6. Ahora os identificais y indicais el NUA, con esta sintaxis:

Nuuuuuuuuuu/pppppp-2120423214

7. Y si todo es correcto aparecera: 'COM.' y despues conectareis sin problemas.

Uso el 048 porque es el mas barato, pero tambien podeis usar el 047.

Si el metodo falla puede que el NUI-password que teneis no sea correcto o sea antiguo, o tal vez Telefonica haya cambiado de nuevo la sintaxis, ya que suele hacerlo bastante a menudo. (Con lo cual tendreis que averiguar la nueva forma de identificacion)

III) El tercer metodo es el mas recomendable para los hackers, ya que no hace falta contratar una cuenta con telefonica.

El problema es que usa el metodo de cobro revertido, que algunos hosts no aceptan con lo que nuestro campo de accion queda mermado. (Y ademas la llamada es mas cara) Aun asi teneis un numero practicamente ilimitado de ordenadores a los que acceder.

El proceso es muy sencillo y seguramente os sonara.

1. Coger un programa de comunicaciones.
2. Seleccionar los parametros de comunicacion a 7El y emulacion de terminal tipo VT100.

Como veis el proceso es similar al acceso con NUI pero a partir de aqui cambia.

3. Marcar del 047 (ATDT047)
4. Cuando se realice la conexion (CONNECT) teclear dos puntos: '..'
5. Aparecera el prompt: 'IBERPAC<'
6. Ahora tecleais le NUA del ordenador al que querais conectaros y YASTA!

2120423214

7. Y aparecera la palabrita 'COM.' y conectareis.

Ejemplo:

```
-----
                                (atdt048)
CONNECT 9600 REL/V42
                                (..)
IBERPAC<
                                (2120423214)
<120423214

COM.
-----
```

Este tercer proceso usa el metodo de llamada a cobro revertido a traves del 047 que como vereis en la tabla de precios que he puesto arriba es algo mas caro que el 048.

Tambien se puede usar el 048 pero la mayor parte de las veces os respondera con el mensaje de que el NUA no acepta llamadas a cobro revertido.

Yo uso como NUA de prueba este: 2120423214 que pertenece a la Biblioteca de la Universidad Autonoma de Madrid. Es de acceso publico y solo tendreis que teclear como Username: BIBLIOTECA para probar si la conexion es correcta.

Mensajes de Iberpac  
=====

Estos son los mensajes que recibireis normalmente de vuestro PAD. Normalmente van acompañados de un numero de tres cifras que indica el codigo del mensaje.

Ejemplo:

```
-----
CLR RNA 000
CLR NP 000
```

CLR ERR 016

-----

COM = Conectado.

CLR RPE = Error en sistema Remoto.

CLR ERR = Error (o sistema punto a punto).

CLR NUI = Error en el NUI/Password.

CLR DTE = El host nos ha expulsado.

CLR INV = Invalido.

CLR OCC = Ocupado.

CLR DER = Fuera de servicio.

CLR NA = No tenemos acceso con nuestro NUI.

CLR NP = El NUA no existe.

CLR NC = Congestion en la red.

CLR CONF = Nuestra peticion de limpiar el PAD ha sido ejecutada.

CLR RNA = No admite cobro revertido

Para que sirve?

=====

Pues a partir de ahora juega tu imaginacion y tu capacidad como hacker, las posibilidades son ilimitadas. Abundan los sistemas antiguos, ordenadores casi imposibles de encontrar en internet en Iberpac se encuentran a montones.

Ademas a traves de Iberpac se puede acceder a la mayoría de las redes publicas X25 de todo el mundo con lo cual el ambito de accion es infinito.

Ni que decir que Iberpac es todavia usada ampliamente por Bancos, Ministerios, Telefonica, etc... objetivos muy atractivos. Sin olvidar por supuesto la famosa linea de seguridad de las cabinas telefonicas o los cajeros automaticos.

Aunque tampoco hay que olvidar que el gran hermano nos esta observando, y la seguridad en Iberpac es bastante alta asi que andaros con cuidado ahi fuera.

Saludos

El Nuevo Eljaker

"Nosotros los estudiamos, nosotros lo controlamos"

EL DUKE DE SICILIA

\*EOF\*

-----  
Aqui teneis una lista casi completa de todos los puntos del nuevo Codigo Penal que afectan directa o indirectamente a los delitos informaticos o tecnologicos, incluyendo hacking y phreaking principalmente.  
-----

NUEVO CODIGO PENAL

TITULO X

Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

CAPITULO I

Del descubrimiento y revelacion de secretos

Articulo 197

1. El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electronico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios tecnicos de escucha, transmision, grabacion o reproduccion del sonido o de la imagen, o de cualquier otra señal de comunicaci on, sera castigado con las penas de prision de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondran al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de caracter personal o familiar de otro que se hallen registrados en ficheros o soportes informaticos, electronicos o telematicos, o en cualquier otro tipo de archivo o registro publico o privado. Iguales penas se impondran a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondra la pena de prision de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imagenes captadas a que se refieren los numeros anteriores. Sera castigado con las penas de prision de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilicito y sin haber tomado parte en su descubrimiento , realizare la conducta descrita en el parrafo anterior.

4. Si los hechos descritos en los apartados 1 y 2 de este articulo se realizan por las personas encargadas o responsables de los ficheros, soportes informaticos, electronicos o telematicos , archivos o registros, se impondra la pena de prision de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondra la pena en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de caracter personal que revelen la ideologia, religion, creencias, salud, origen racial o vida sexual, o la victima fuere un menor de edad o un incapaz, se impondran las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondran las penas respectivamente previstas en los apartados 1 al 4 de este articulo en su mitad superior. Si ademas afectan a datos de los mencionados en el apartado 5, la pena a imponer sera la de prision de cuatro a siete años.

## Artículo 198

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

## Artículo 199

1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

## Artículo 200

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este código.

## Artículo 201

1. Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquella sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4º del artículo 130.

## Artículo 248

1.- Cometan estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

## Artículo 249

Los reos de estafa serán castigados con la pena de prisión de seis meses a

cuatro años, si la cuantía de lo defraudado excediere de cincuenta mil pesetas. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre este y el defraudador, los medios empleados por este y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción.

#### Artículo 256

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a este un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

#### Artículo 263

El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si este excediera de cincuenta mil pesetas.

#### Artículo 264

1.- Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriera alguno de los supuestos siguientes:

- 1).- Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.
- 2).- Que se cause por cualquier medio infección o contagio de ganado.
- 3).- Que se empleen sustancias venenosas o corrosivas.
- 4).- Que afecten a bienes de dominio o uso público o comunal.
- 5).- Que arruinen al perjudicado o se le coloque en grave situación económica.

2.- La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

### CAPITULO XI

De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores

#### Sección 1ª.- DE LOS DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL.

#### Artículo 270

Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero,

reproduzca, plagie, distribuya o comunique publicamente, en todo o en parte, una obra literaria, artistica o cientifica, o su transformacion, interpretacion o ejecucion artisitica fijada en cualquier tipo de soporte o comunicada a traves de cualquier medio, sin la autorizacion de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. La misma pena se impondra a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorizacion. Sera castigada tambien con la misma pena la fabricacion, puesta en circulacion y tenencia de cualquier medio especificamente destinada a facilitar la supresion no autorizada o la neutralizacion de cualquier dispositivo tecnico que se haya utilizado para proteger programas de ordenador.

#### Articulo 278

1.- El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electronicos, soportes informaticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos sealados en el apartado 1 del articulo 197, sera castigado con la pena de prision de dos a cuatro años y multa de doce a veinticuatro meses.

2.- Se impondra la pena de prision de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3.- Lo dispuesto en el presente articulo se entendera sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destruccion de los soportes informaticos.

#### Articulo 279

La difusion, revelacion o cesion de un secreto de empresa llevada a cabo por quien tuviere legal o contractualmente obligacion de guardar reserva, se castigara con la pena de prision de dos a cuatro años y multa de doce a veinticuatro meses. Si el secreto se utilizara en provecho propio, las penas se impondran en su mitad inferior.

### CAPITULO III

#### Disposicion general

#### Articulo 400

La fabricacion o tenencia de utiles, materiales , instrumentos, sustancias, maquinas, programas de ordenador o aparatos, especificamente destinados a la comision de los delitos descritos en los capitulos anteriores, se castigaran con la pena sealada en cada paso para los autores.

#### Articulo 536

La autoridad, funcionario publico o agente de estos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios tecnicos de escuhas, transmision, grabacion o reproduccion del sonido, de la imagen o de cualquier otra señal de comunicacion, con violacion de las garantias constitucionales o legales, incurrira en la pena de inhabilitacion especial para empleo o cargo publico de dos a seis años. Si divulgare o revelare la informacion obtenida, se impondran las penas de inhabilitacion especial, en

su mitad superior y, ademas la de multa de seis a dieciocho meses.

Articulo 623

Seran castigados con arresto de dos a seis fines de semana o multa de uno a dos meses:

- 4). Los que cometan estafa, apropiacion indebida, o defraudacion de electricidad, gas, agua u otro elemento, energia o fluido, o en equipos terminales de telecomunicacion, en cuantia no superior a cincuenta mil pesetas.

-----Recopilado de varias fuentes por Dark Raver-----

\*EOF\*

```
*****
* PUERTOS *
*****
```

Por VaLfAdIr.

Hola a todos.

Aunque es muy probable que la mayoría de vosotros ya lo sepais, voy a daros una relación de puertos de hosts, a los que se puede acceder (si no están deshabilitados) y os dare algunos ejemplos y utilidades interesantes que se pueden sacar con esto.

Todos los hosts que están en La Red están configurados para dar una serie de servicios a los usuarios que se conectan a ellos. Estos servicios están asociados con los puertos, es decir cuando habilitas el servicio TIME, estás habilitando el puerto 37. De esta manera puedes acceder al servicio TIME a través del puerto 37.

Los puertos se pueden considerar como las puertas de entrada a los servicios de un hosts. Por ejemplo, cuando accedemos a las páginas Web de un hosts nuestro navegador, además de otras muchas cosas, está accediendo al puerto 8000 que es el puerto del servicio HTTP.

“Y para que sirve todo esto? Bueno puede que para nada, o puede que para mucho. Lo interesante de esto es que puedes acceder a cualquiera de estos puertos (siempre que estén habilitados) con un simple telnet. Cuando haces un telnet por defecto se conecta al puerto 23, que es el servicio de telnet, pero tu le puedes decir que se conecte a otro puerto.

Ejem.: telnet objetivo.com 110

En este ejemplo le hacemos un telnet al host objetivo.com por el puerto 110, que es el puerto del servicio POP3. Os aparecerá en pantalla algo como esto:

```
+OK Welcome to objetivo.com POP3 Server
```

Muy bonito, “y que?. Bueno pues resulta que si ahora pones:

```
user valfadir (tu login)
```

Te responderá:

```
+OK Password required for user "valfadir"
```

Ahora pones tu password con:

```
pass ***
```

Te responderá esto:

```
+OK valfadir has 6 messages (49450 octets).
```

Y si ahora tecleas:

```
list
```

Pues te aparecerán una lista en forma de dos columnas de números, la primera corresponde al orden secuencial de los mensajes y la segunda es el número identificador del mensaje. Estos son los mensajes nuevos que no has leído. Algo parecido a esto:

```
+OK 6 messages (49450 octets)
```

1 8661  
2 4888  
3 2093  
4 4171  
5 26799  
6 2838  
.

Normalmente el mensaje cuyo identificador es de 5 digitos quiere decir, o bien que el mensaje es muy largo, o que tiene enganchado algun fichero.

Incluso puedes leerlos, sin bajartelos. Poniendo lo siguiente leerias el primero:

top 1 8661

No se si os parecera util, a mi me resulta muy util. Sobre todo si tienes varias cuentas de correo. Tambien es muy util si sospechais que os ha hecho un mail-bombing, os conectais al puerto 110, listais los mensajes y si hay tropecientosmil, pues llamais a vuestro proveedor y que los borre.

Tambien es muy util para el que tiene una cuenta en hotmail, en vez de acceder por Web (mucho mas lento que un telnet), utilizais este metodo. Por supuesto tambien podeis configurar vuestro navegador para bajaros directamente el correo de hotmail sin tener que acceder por Web. Y esto es posible gracias a que tiene habilitado el famoso puerto 110 (POP3).

Alguna mente malevola ;-), ya se le habra ocurrido alguna cosilla. Tened en cuenta que no bajamos el correo a nuestro ordenata, solo lo consultamos.

Tambien es muy interesante el acceso al puerto 25 (SMTP). Desde aqui podeis mandar mensajes pseudoanonimos (no son anonimos puros, es decir que no os paseis ya que os pueden rastrear por la IP), pero esta bien para gastar alguna bromilla, siempre y cuando la victima no se entere mucho. Ya que mirando las cabeceras del mensaje se puede hacer una idea.

Otra utilidad es para conocer la verdadera identidad de una cuenta de correo. Imaginad que os mandan un mensaje un tal reficul@inferno.com y quereis saber el verdadero nombre de este tio. Bueno pues haceis esto:

telnet inferno.com 25

Os saldra algo parecido a esto:

220 inferno.com ESMTP Sendmail 8.8.5/8.8.5; Tue, 2 Sep 1997 16:43:01 -  
0600 (CST)

Y luego poneis:

vrfy reficul

Y os podria aparecer:

250 Ibon Zaramendia Mentxaka <reficul@mail.inferno.com>

Esto siempre no funciona, y cada vez menos aunque todavia quedan muchos. Tambien tened en cuenta que una cuenta puede tener dos direcciones de correo para dos personas diferentes, este comando siempre os va a dar la identidad de la persona que ha contrado la cuenta con el proveedor. Osea que si el mensaje os lo ha mandado la segunda persona (con la segunda direccion de correo) la identidad no va a coincidir.

Bueno aqui os dejo una relacion de puertos. Seguramente faltan algunos o muchos, he intentado poner los mas comunes. Para que os hagais una idea, yo utilizo un programa para escanear puertos llamado UltraScan y por defecto escanea desde el puerto 1 al puerto 1024, por supuesto lo puertos habilitados en un hosts no tienen por que ser secuenciales.  
Practicar, es muy interesante.

113	AUTH	531	CONFERENCE
530	COURIER	13	DAYTIME
9	DISCARD	53	DOMAIN
7	ECHO	520	EFS
512	EXEC	79	FINGER
21	FTP	101	HOSTNAMES
8000	HTTP	1524	INGRESLOCK
87	LINK	513	LOGIN
57	MTP	42	NAMESERVER
532	NETNEWS	15	NETSTAT
119	NNTP	109	POP2
110	POP3	17	QOTD
556	REMOTEFPS	77	RJE
115	SFTP	514	SHELL
25	SMTP	515	SPOOLER
111	SUNRPC	95	SUPDUP
11	SYSTAT	23	TELNET
526	TEMPO	37	TIME
540	UUCP	117	UUCP-PATH
	43	WHOIS	

Bueno pues esto es todo, si os ha resultado interesante y al e-zine le parece bien, escribire algo sobre los servicios POP3 (port 110) y SMTP (port 25) en concreto.

Hasta la proxima.

#VaLfAdIr#

Si la puerta esta cerrada...  
--- TIRALA !!!  
Y libera la informacion.

\*EOF\*

## Codigos de Barras

Por Warezzman

warezzman@usa.net

-&gt; Introduccion

Estamos en la era de la informacion, estamos sumergidos en ella, esta informacion contribuye a (o quiza controla?) nuestra vida, los datos se encuentran codificados en casi cualquier sitio, tarjetas telefonicas, tarjetas magneticas, tarjetas inteligentes, y codigos de barras...

Mira un momento a un alrededor, seguro que hay algun codigo de barras en alguna cosa junto a ti, puede que incluso decenas...

Te has preguntado alguna vez como funcionan? para que sirven? o quiza has pensado alguna vez si se podrian usar en tu "provecho personal" ?

-&gt; Los Codigos de Barras (CB)

Los codigos de barras son en primer lugar una forma optica para almacenar informacion reconocible por sistemas informaticos.

Se usan en sistemas de control de acceso, manejo automatizado de objetos, pero quiza los mas conocidos son los usados para identificar productos de consumo, de estos ultimos se hablara en este articulo.

Si quieres seguir mejor este articulo busca un CB y observalo....

Facilmente puedes distinguir dos partes diferencaidas, el CB es si mismo y un numero en la parte inferior. Cuenta las cifras de este numero...

"tiene 13 cifras verdad? Eso es por que los CB siguen un standard llamado EAN-13 (EAN = European Article Numbering)....

"como, que no tiene 13 cifras????? el EAN13 es el sistema mas comun en europa pero hay otros, el UPC (originario de USA) o el EAN8 que pese a ser minoritarios tambien se pueden encontrar en nuestro pais.

Pero sigamos esas rayas que forman el CB son la codificacion optica del numero que esta a su lado, ese numero es por decirlo de alguna manera el DNI del producto, lo identifica como tal.

Cuando realizas una compra, la amable cajera pasa el CB del productos comprado por un scanner, de forma automatica el numero representado en el CB es comparado con los almacenados en la base de datos y el importe de contabiliza de manera inmediata.

Los CB aportan una gran cantidad de ventajas a los vendedores, algunos ejemplos son: seguimiento en tiempo real del volumen de ventas, rapidez de atencion al cliente, eliminacion de la posibilidad de error en el mercado, ahorro de tiempo y dinero en etiquetado, etc, etc

-&gt; EAN13

En el EAN13 se usa un digito de control para evitar posibles fallos de lectura en el CB, este digito de control es el ultimo digito del CB y el que se encuentra mas a la derecha. Se calcula de la siguiente manera:

1. Se suman los valores de los digitos en las <posiciones> pares esto es  $A=0+2+4+6+8+10$
2. Se suman los valores de los digitos en las <posiciones> impares osea  $B=1+3+5+7+8+11$  y el valor resultante se multiplica por 3 ( $B*3$ )
3. Se realiza la suma de los resultados anteriores  $C=A+B$
4. Se calcula el modulo 10 de C, si el resultado no es 0 se resta de

10 y el numero resultante es el codigo de integridad.

Ejemplo: CD-Recordable TraxData 74m. Su codigo es 5030159000106

```
Suma de las posiciones pares  5 + 3 + 1 + 9 + 0 + 1 =      19
Suma de las posiciones impares 0 + 0 + 5 + 0 + 0 + 0 = 5 * 3 = 15
                                     -----
                                     34
```

34 MOD 10 = 4    10 - 4 = 6 <----- DIGITO DE CONTROL

El resto de las cifras tienen tambien su significado, las 2 primeras identifican el pais de origen de la marca. En españa la entidad gestora del EAN13 es AECOC, los codigos de las empresas asociadas a AECOC tienen este formato:

```
00 01 02 03 04 05 06 07 08 09 10 11 12
-- -- -- -- -- -- -- -- -- -- -- -- --
 8  4 X1 X2 X3 X4 X5 X6 X7 X8 X9 X10 DC
```

84 Es el prefijo asignado por EAN internacional a AECOC. Esto no quiere decir necesariamente que sea un producto fabricado en españa sino simplemente que la empresa fabricante usa un CB asignado por AECOC.

X1..X5..X8 En este espacio aparece el codigo asignado por AECOC a la empresa propietaria de la marca del producto. Dicho codigo tendra entre 5 y 8 digitos dependiendo de las necesidades de la empresa.

X6..X9.X10 Este espacio es utilizado por la empresa fabricante para identificar cada producto en particular. El posible espacio sobrante se corrige añadiendo los ceros necesarios a la izquierda.

DC es el digito de control calculado con la formula vista antes.

```
Ej. Gallina blanca, Sopinstant, Crema de champiñones 8 410300 100751
     Gallina blanca, Sopinstant, Pollo con pasta      8 410300 100799
```

Pasemos ahora a la parte quizas mas farragosa de los CB: la representacion optica del codigo en forma de barras. Como esta pasa por ser bastante complicada solo la comentare por encima, si estais realmente interesados en conocer como funciona podria escribir una segunda parte de este articulo.

En primer lugar el CB esta dividido en 2 segmentos, que agrupan cada uno a 6 digitos y forman en pareja los 12 digitos del cb, delimitados por las lineas mas largas de los extremos y centro. En el CB una barrita fina significa 1 y una en blanco 0. De esta forma las barras de calibrado dan lugar a los valores 101 en los extremos y 01010 en el centro. Los segmentos codifican los grupos de 6 cifras usando 3 tablas de codigos de 7 bits que a su vez dependen de una tabla de patrones de manera que segun el valor del digito de control se use un patron u otro.

-> (IN)Seguridad de los codigos de barras

Silogismo de los codigos de barras:

- 1 - Un CB es parte de un sistema informatico
- 2 - TODO sistema informatico se puede hackear/crackear

De lo que deducimos que: "Un CB se puede hackear/crackear"

"Acaso no te has dado cuenta de que cuando compras algo en el super de

la esquina la informacion sobre el precio del producto se extrae del CB?

Supongamos por un momento que imprimes un CB identico a una botella de vino del "Tio de la bota" y la pegas en una cara botella de vino frances cosecha del 89, la cajera pasara el cb por el scanner y en la pantalla aparecera "vino" y pagaras 130pts por una botella que vale 5000pts.

Ojo todo esto es hipotetico, debe quedar claro que no pretendo incitar a cometer un delito, simplemente expongo las deficiencias de seguridad de los CB. ;-)

Continuemos suponiendo, nada te impediria comprar una SB AWE 64 GOLD al precio de la 32 Value Edition. Veamos que pasos deberias seguir para "perpetrar" este tipo de acciones:

- Anotar el codigo de un producto similar al que nos vamos a llevar y de un precio inferior, es recomendable comprobar que tal producto se encuentra a la venta en el lugar en cuestion.
- Imprimir en casa sobre una etiqueta adhesiva el cb correspondiente, existen multiples programas tanto shareware como comerciales para estos menesteres, y en inet no es dificil encontrar alguno de ellos.
- Pegar dicha etiqueta sobre la original y pasar por caja.

Si vas de "Hacker con buenas intenciones" puedes imprimir el mismo codigo que el original para demostrarte a ti mismo que podrias haber defraudado al sistema si hubieras querido, en algunas grandes superficies incluso hay lectores de CB a disposicion del publico para que comprueben el precio de los productos, ya que este no va etiquetado en el envase.

Para finalizar agradecer a +ORC por la informacion original "How to crack barcodes" y a KazMeyer. Sed buenos y no hagais nada que yo no haria. }:)

\*EOF\*



asi hasta llegar hasta la ultima fila. Si eres tan paranoico como para hacer un scaneo aleatorio, te sera facil pues veras visualmente cuales son los numeros que llevas marcados y cuales te quedan por marcar.

Saludos, y prosperos scanneos.

\*EOF\*

Ya se que llega un poco tarde pero aqui teneis el esperado reportaje sobre la UnderCon 97.

Supongo que habreis oido noticias sobre este congreso nacional de hackers, no fue totalmente nacional porque hubo un boicoteo por parte de gente de algunas regiones, pero bueno eso son tonterias...

Fue el ultimo fin de semana de octubre y se celebro en la capital del hacking levantino: Murcia.

Vino gente de Madrid, Alicante, Granada e incluso desde Leon (casi 1000km.) que unidos a la gente de Murcia llegaron a ser mas de 50 o 60 personas.

En contra de lo que algunos poco-solidarios (Por no llamarles otra cosa) estuvieron diciendo, la gente que vino al congreso tenia mucho nivel... nada de lamers, nada de novatos, solo hackers y phreakers...

Vino gente de la Vieja Guardia, Saqueadores, CPNE, La Katedral, incluso de Hispahack...

Hubo conexion telefonica (Gracias a las Calling cards :) con la gente de Cyberhack que no pudieron asistir, y tambien se unieron a traves del irc gente de saqueadores de la zona norte.

La pena fue no contar con nadie de cataluña, hay gente muy buena por alli, pero segun parece se corrio un rumor falso y mucha gente se lo creyo.

Parece que hay algunos piques personales que estan estropeando el buen ambiente de la escena hack española.

Durante los tres dias del congreso se hablo de muchos temas, pero destaco sobre todo el phreaking. Los chicos de la CPNE eran unos de los anfitriones y practicamente monopolizaron los temas de conversacion :-)

Se hablo mucho de los 900 con acceso a internet de IBM, de Samsung e incluso de los de Telefonica y Microfost...

Tambien se hablo de las trajetas chip (smartcards)

Se hablo de hacking, como no. El articulo de los ascend de paseante fue la estrella.

Tambien se hablo bastante de linux, para que os hagais una idea el 90% de los asistentes eran usuarios de linux, un buen sintoma...

Por supuesto no faltaron las criticas a Microsoft y a Telefonica.

La dudosa seguridad de los NTs y del protocolo NetBios fueron base para muchos chistes...

El dia grande fue el sabado, se junto tanta gente que incluso hubo personas a las que tenia ganas de saludar y ni siquiera las vi... :) perdona Case Zer0 a ver si podemos hablar mas el año que viene...

La organizacion fue bastante mala... pero es comprensible la primera vez y con prisas... Aun asi gracias al buenisimo nivel de la gente que vino se salvo la cosa...

Los objetivos del evento se cumplieron, se establecio un contacto entre los componentes de la escena hack/phreak y se sentaron las bases para futuras convenciones.

Lista de asistentes:

Dark Raver / Saqueadores / CPNE  
Entropia  
Warezzman / Saqueadores / CPNE  
Darkcode / Vieja Guardia  
Necronoid / Vieja Guardia / Hispahack  
FastData / CPNE  
Flecha  
Dairo Bel / Vieja Guardia  
Fuego Fatuo  
Fit0 / Vieja Guardia / Hispahack  
Overdrive / Net Phreak team  
Shou  
\_Sauron  
Mainboard  
Gotcha  
Fateros  
Ufo  
Pipo  
Netdancer  
Jcl  
Pleyade  
Pesca  
Senpai  
GuyBrush / Raregazz  
Cain Garcia  
Ric3  
Kloniko  
Kemo  
Lord\_lt  
Axel  
D\_hunter  
Bishop  
CaseZer0  
Eljaker / Saqueadores

Algunos se escaparon sin firmar, pero como podeis ver la cosa estuvo muy bien.

Tampoco firmaron los 3 chicos de seguridad de Telefonica que se pasaron por alli "de incognito" preguntando por los ascend... :) paseante cuidadin que van a por ti!!

De las actividades que estaban planeadas solo se cumplieron dos:

-Se repartio una saqueadores especial, no era nada espectacular pero habia un par de articulos buenos... Conseguir una copia esta bastante dificil, se puede decir que incluso fue una edicion de coleccionistas :)))

-Finalmente y en un tiempo record se pudieron hacer camisetas... y como se hicieron poas pues faltaron y mucha gente se quedo con las ganas... una pena.

--> Por cierto ni se os ocurra lavarlas porque destinen :)))

Y aqui teneis un pequeño texto que se escribio alli mismo, y en que colaboraron entre otros \_Sauron, Warezzman, Dairo, Fastdata y algunos mas que estaban demasiado borrachos para recordar su propio apodo :)

-----  
Celebramos en Murcia la Undercon '97, y es, resumiendo en dos palabras:  
"Im-prezionante". Pretendemos asentar las bases para futuras "jornadas para trabajo y estudio de seguridad informatica"

Mencion especial tuvo nuestra querida y no siempre bien ponderada Timofonica, de la cual se hablo largo y tendido, aportandose ideas, experiencias y nuevas "lineas de trabajo".

Supongo que dichas ideas no seran aplaudidas precisamente por "el monopolio". Agradecemos la presencia de representantes de nuestra querida amiga en plan Bond 007.

Como no podia ser de otra manera el hack fue invitado de excepcion.

Resumiendo undercon '97 ha sido segun los asistentes un punto de encuentro del underground español, con la pretension de que este tipo de iniciativas tengan una continuidad y que sirvan para mejorar nuestros conocimientos sobre todo tipo de sistemas.

En un principio reinaba la anarkia al igual que en nuestra querida red. Organizandose de forma espontanea y rompiendo el hielo entre los distintos grupos.

Los participantes decidieron que SIMO'97 seria una buena oportunidad para un nuevo encuentro...

La organizacion agradece especialmente la participacion de los miembros de los siguientes grupos:

- Hispahack
- Vieja Guardia
- CPNE
- katedral
- Etc...

-----  
\*EOF\*