———————————————————

By QuasaR - UNDERSEC Security Team

Revision 22-Diciembre-2000*

1 INTRODUCCION

Alla por marzo del 96 la compañia 3com se invento una aparatito de lo mas curioso que cumplia perfectamente las labores de la agenda electronica aparecida años antes (vease casio) pero que ademas iba mas alla con caracteristicas mas acercadas a las necesidades de hoy en dia. La politica le ha funcionado bien, porque el numero de ventas de Palms se ha ido incrementando notablemente, al igual que se han ido ampliando las posibilidades y caracteristicas de estos dispositivos.

Una de las posibilidades mas grandes que ofrecen las palm pilot es su posibilidad de interconexion independientemente del Hardware o OS el que la deseemos conectar. Si alguien sabe de las mismas posibilidades con pocketwin que me envie un email.

Los textos sobre palm pilot (& howto's) que podemos encontrar por ahi, en su mayoria en ingles, nos tocaran temas muy concretos. Basados principalmente en instalacion & programacion de aplicaciones sobre palm. Por lo que echando un detenido vistazo me he decantado por este texto (mini-howto a fin de cuentas) sobre interconexion de la palm, mucho menos documentado en ingles y casi cero en castellano.

2 SINCRONIZACION

Una de las posibilidades inicales que ha traido palm desde siempre ha sido el proceso de sincronizacion. Es el proceso mediante el cual es posible realizar instalacion & backups de la palm al ordenador y viceversa mediante el cradle o base. No existe ningun misterio bajo plataforma windows, mas que nada porque el software que trae la propia palm en su caja, ya es mas que suficiente para abastecer todas lasñecesidades de sincronia de la palm. Ademas en la propia pagina de Palm (http://www.palm.com) esta disponible todos los updates de este sofware para plataformas windows.

*Original: 25 - Octubre - 2000. 1ª Revision: 22 Diciembre - 2000

El tema se vuelve un pelin mas exigente para plataformas Linux y FreeBSD. Para ambos existen un paquete de utilidades+librerias para una correcta sincronizacion, tanto en modo consola como en modo grafico.

No he probado utilidades como Kpilot (http://www.slac.com/pilone/kpilot_home/) y similares sobre entorno grafico. Lo que si esta claro es que ofrecen mayor comodidad y ciertas mejoras sobre las de consola. Entre ellas la posibilidad de realizar la mayoria de las operaciones desde un mismo programa (no asi en consola). Y la posibilidad de dejar en segundo plano un applett que reconozca la pulsacion del boton de sincronia de la base y realice el proceso automaticamente.

Para consola en este apartado tenemos las pilot-link (ftp://ryeham.ee.ryerson.ca/pub/PalmOS/). Un paquete de herramientas bastante completo. El problema es que segun lo que queramos hacer necesitaremos de un programa u otro. Aunque las posibilidades son practicamente, quitando algunos detallitos, las mismas que sobre la plataforma windows.

Para informacion mas detallada sobre las pilot-link hay ya que leerse las man (man pilot-link) una vez instalado el paquete. Existe tambien el port con el patch para versiones de FreeBSD q funciona correctisivamente.

Solo nombrar aki un par de detalles facilmente pasables por alto. A partir del Palm OS 3.3 la sincronia se puede realizar a una velociadad de 57600. En windows accediendo a un simple menu es posible variar la velocidad. Para linux y FreeBSD hay que asignar un valor a una variable de entorno:

```
export PILOTRATE=57600 (o la velocidad que deseemos)
```

El segundo es tambien para plataformas linux & FreeBSD. Es muy recomendable un simbolico al serie donde tengamos la palm metida:

```
Linux:
      ln -s /dev/pilot /dev/ttyS0 (o ttyS1)
FreeBSD:
      ln -s /dev/pilot /dev/ttyd0 (o ttyd1)
```

Para mas informacion sobre sincronia hay que buscar ya en sitios oficiales (http://www.palm.com) o menos oficiales (http://www.handango.com)

Y ahora pasamos a una de las opciones mas interesantes de palm...

3 CONEXION PPP

La palm lleva una pila TCP/IP bastante resumida pero con enormes posibilidades y ademas es capaz de soportar conexiones punto a punto. Ya sea con un modem, a traves de IR (IRDA) sobre un movil (o portatil) o bien al serie de otro

equipo.

La interconexion de la palm al movil/modem nos da la posibilidad de acceder a cualquier sitio desde cualquier lugar que nos encontremos mientras tengamos cobertura. Existen clientes de telnet, web, wap, vnc, correo.... para poder consultar lo que queramos.

La interconexion de la palm desde otro ordenador por ejemplo es mas discutida. Para que queremos usar la palm, si ya tenemos el ordenador? Pues nunca se sabe. En casa de un amigo que el tio esta ocupando el ordenador todo el rato. O en

una party o en una reunion.... el caso es que tenemos un acceso transparente desde ese ordenador al resto de la red o internet.

Y ahora nos vamos a centrar en este segundo punto:

3.1 Conexion ppp + palm + windows

La conexion de la palm a traves de plataformas windows es muy sencilla. Todo se resume a bajarse el programilla Mochappp (http://www.mochasoft.dk) y configurarlo, sin ningun misterio, adecuadamente. El programa espera una

conexion ppp de la palm y le asigna la ip y las dns que posee a la palm. De esta forma la palm es completamente transparente a todo y todos. Ya veremos que no ocurre lo mismo en otras plataformas, donde la palm se

comportara como una maquina mas. Tan solo hay que tener en cuenta que en el menu de configuracion de red de

la palm:

```
Prefer (preferencias) -> Red -> Detalles
```

Debemos seleccionar que todo este asignado automaticamente y en PPP. En windows 98 el Mochappp con Palm OS 3.3 funciona perfectamente.

Otra cosa que tambien recalcare mas adelante, es que esta posibilidad de conexion ppp a velocidades por encima de 19200 es viable siempre que se tenga el OS 3.3 o superior. En caso de no ser asi, existe la utilidad linkdirect.prc

(http://http://www.vmlinuz.org/palmos/linkdirect.html) para palm que soluciona esta decadencia en Palm OS anteriores. Yo tuve la posibilidad de probarlo con OS 3.0 y salvo evolucion, el programa es de dudoso funcionamiento. Iba cuando queria. Pero bueno, es lo que hay.

3.2 Conexion ppp + palm + linux

Llegamos a plataformas Linux. Las pruebas se realizaron sobre debian y un 2.2.17 y todo funciona perfectisimanente.

Para poder realizar la conexion ppp necesitaremos tener habilitado el forwarding y el masquerade en nuestro sistema.

Habra que tener compilado en el kernel o como modulo todo lo relacionado con el forwarding y el masquerade. Ejemplillo de turno:

```
#
#Ñetworking options
#
# CONFIG_CIPE isñot set
CONFIG_PACKET=y
```

```
CONFIG_NETLINK=y
CONFIG_RTNETLINK=y
CONFIG_NETLINK_DEV=m
CONFIG_FIREWALL=y
# CONFIG_NET_SECURITY isñot set
# CONFIG_FILTER isñot set
CONFIG_UNIX=y
CONFIG_INET=y
# CONFIG_IP_MULTICAST isñot set
CONFIG_IP_ADVANCED_ROUTER=y
CONFIG_RTNETLINK=y
CONFIG_NETLINK=y
CONFIG_IP_MULTIPLE_TABLES=y
CONFIG_IP_ROUTE_MULTIPATH=y
# CONFIG_IP_ROUTE_TOS isñot set
CONFIG_IP_ROUTE_VERBOSE=y
# CONFIG_IP_ROUTE_LARGE_TABLES isñot set
CONFIG_IP_ROUTE_NAT=y
# CONFIG_IP_PNP isñot set
CONFIG_IP_FIREWALL=y
# CONFIG_IP_FIREWALL_NETLINK isñot set
# CONFIG_IP_ROUTE_FWMARK isñot set
CONFIG_IP_TRANSPARENT_PROXY=y
CONFIG_IP_MASQUERADE=y
# CONFIG_IP_MASQUERADE_ICMP isñot set
# CONFIG_IP_MASQUERADE_MOD isñot set
# CONFIG_IP_ROUTER isñot set
# CONFIG_NET_IPIP isñot set
# CONFIG_NET_IPGRE isñot set
CONFIG_IP_ALIAS=y
# CONFIG_ARPD isñot set
CONFIG_SYN_COOKIES=y
# CONFIG_INET_RARP isñot set
CONFIG_SKB_LARGE=y
# CONFIG_IPV6 isñot set
# CONFIG_IPX isñot set
# CONFIG_ATALK isñot set
# CONFIG_X25 isñot set
# CONFIG_LAPB isñot set
# CONFIG_BRIDGE isñot set
# CONFIG_LLC isñot set
# CONFIG_ECONET isñot set
# CONFIG_WAN_ROUTER isñot set
# CONFIG_NET_FASTROUTE isñot set
# CONFIG_NET_HW_FLOWCONTROL isñot set
# CONFIG_CPU_IS_SLOW isñot set
```

Ahora y despues de recomilar hay que activar la opcion del forwarding:

```
echo '1' > /proc/sys/net/ipv4/ip_forward
```

Y cargar los modulos pertinentes segun el servicio que vayamos a usar....

```
cd /lib/modules/2.2.1x/ipv4
```

Ahi tenemos todos los modulos de los servicios a enmarcarar. Ejemplillo de turno:

```
-rw-r--r--  1 root     root        11308 Oct 25 15:26 ip_gre.o
-rw-r--r--  1 root     root         4832 Oct 25 15:26 ip_masq_autofw.o
-rw-r--r--  1 root     root         2632 Oct 25 15:26 ip_masq_cuseeme.o
-rw-r--r--  1 root     root         4888 Oct 25 15:26 ip_masq_ftp.o
-rw-r--r--  1 root     root         3548 Oct 25 15:26 ip_masq_irc.o
-rw-r--r--  1 root     root         6276 Oct 25 15:26 ip_masq_mfw.o
-rw-r--r--  1 root     root         4904 Oct 25 15:26 ip_masq_portfw.o
-rw-r--r--  1 root     root         3216 Oct 25 15:26 ip_masq_quake.o
-rw-r--r--  1 root     root         5260 Oct 25 15:26 ip_masq_raudio.o
-rw-r--r--  1 root     root         5244 Oct 25 15:26 ip_masq_user.o
-rw-r--r--  1 root     root         3080 Oct 25 15:26 ip_masq_vdolive.o
-rw-r--r--  1 root     root         9324 Oct 25 15:26 ipip.o
```

Hay que cargar el que queramos (modprobe). Una vez cargados los modulos correspondientes tenemos que activar el
enmascaramiento (masquerade). Bastara con:

```
ipchains -A forward -s 0/0 -d 0/0 -j MASQ
```

Si se requiere de un mayor control sobre el masquerade es mejor que os leais cierta documentacion sobre ipchains.

Bien, ahora lo que haremos es crear el server pppd y que espere una conexion punto a punto en el serie que le digamos. La linea de comandos a utilizar seria, en su formato mas basico, algo como:

```
pppd /dev/serie velocidad :ipdepalm parametros
```

Ejemplillo:

```
pppd /dev/pilot 57600 :10.0.0.2 local debug passive crtsctsñoauth
```

/dev/pilot -> pilot es link a nuestro serie

57600 -> velocidad que queramos

:10.0.0.2 -> Aki metemos la ip que la palm va a tener (inventada pero en nuestra misma subred). Es un hecho muy curioso ver como sobre linux la palm se va a comportar como un dispositivo/elemento completamente distinto y que va a formar parte de nuestra red.

local -> lo usamos para que no espere el tono de la linea telefonica.

debug -> muestra todo el proceso de conexion (syslog)

crtscts -> para el control de la comunicacion, la palm lo soporta.

passive -> Cuando el LCP no envia un pakete correcto en vez de salir aguanta hasta un reset by peer.

noauth-> sin solicitar autorizacion par ael uso de la linea ppp.

En principio con estos parametros el server ppp (pppd) deberia de quedar a la escucha. Siempre podremos enriquecer mas nuestro pppd añadiendole mas parametros.

```
pppd /dev/pilot 57600 :10.0.0.2 local debug passive crtsctsñodetach proxyarp auth &
```

nodetach -> para mantener el terminal ocupado mientras se ejecuta pppd

proxy-arp -> asigna una direccion mac a la ip de la palm. A fin de cuentas es una alias de la del ordenador al que esta coenctada.

auth -> Pide autorizacion para el uso de la linea. Utiliza el pap-secrets.

& -> al tener el nodeatch esto hara que se meta en segundo plano ;)

La opcion ms-dns aparece en algunos documentos como valida para asignar unas dns's a la palm (la palm soporta esto), sin embargo no nos funciono por lo que recomiendo asignar manualmente las dns desde la propia palm:

```
Prefer (preferecias) -> red -> detalles --> kitar checkbox de dns autmaticas
```

El siguiente paso es asegurar que las rutas son las correctas. Hay que pensar que vamos a realizar una conexion ppp y que por lo tanto uno de nuestros dispositivos PPPx va a ser usado (sea ppp0 o ppp1... dependiendo de las conexiones punto a punto que tengamos establecidas). En principio, lo adecuado seria que la ruta por defecto de la palm utilizara a nuestra makina de gateway por defecto, y deberia funcionar. Igual lo que viene a continuacion no es necesario. Sin embargo, por las diferentes configuraciones de las rutas estaticas del route puede ser que no haga el acceso hasta internet o no pase mas alla de nuestra makina. Es decir, puede que llegue el caso de que con nuestro ordenador si funcione pero fuera de el

ya no, por culpa del gateway o que los dns son inalcanzables. Ahi van diferentes opciones:

```
route add ipdepalm dev dispositivo gw ipmakina
```

o bien tambien tengamos que reconfigurar la ruta por defecto del gateway.

```
route del gateway
route add gateway dev dispositivo-inet
```

OJO!!!! aki el dispositivo es el de acceso a internet!. No el que la palm va a crear.

ejemplos:

```
route add 10.0.0.2 dev ppp0 gw 10.0.0.1
```

o tambien:

```
route del default
route add default dev ppp0
```

En este segundo caso, ppp0, es el de inet, el de la palm entonces seria de ppp1 en adelante y como pap-secrets de ejemplo:

```
quasar  *  password  *
```

NOTA: los * son necesarios.

Una vez hecho todo esto (muy engorroso de explicar, muy facil de realizar) tendremos una conexion ppp con la palm. Solo hay que darle al connect de la palm para que funcione... Pasemos a la explicacion con FreeBSD y luego expondre datos curiosos y conclusiones....

3.3 Conexion ppp + palm + FreeBSD

La configurracion para la conexion de la palm y la Free es muy similar a la de Linux, pero no igual. De hecho, por la poca documentacion existente casi los mismos pasos han costado un poco mas.

Para empezar, y al igual que en Linux, necesitamos que el kernel traiga soporte para gateway osease, firewalling y forwarding.

```
options  INET  #InterNETworking
options  IPFIREWALL  #packet filtering
options  IPFIREWALL_VERBOSE
#logging of packets through syslogd
options
IPFIREWALL_VERBOSE_LIMIT=10 #num max logging packets
```

El resto de opciones necesarias ya vienen en el fichero de conf del nucleo generico. Las tres ultimas se deben de poner porque con el generico, por lo menos en la version 4.0 de la FreeBSD, no vienen.

En la opcion:

```
options IPFIREWALL_VERBOSE_LIMIT=10
```

el numero seria acertado que estuviere entre 10 y 100.

Ahora creamos el enlace simbolico ya comentado anteriormente:

```
ln -s /dev/pilot /dev/ttyd0 (o ttyd1)
```

Y activamos la opcion de forwarding. Dos maneras:

1. Añadir linea: gateway_enable="YES" al fichero /etc/rc.conf
2. O desde la shell: sysctl -w net.inet.ip.fw.enable=1

La diferencia reside en que con el 1. esta ya para siempre activado, no asi en el 2. que habra que teclearlo cada vez que se encienda el ordenador.

Lo curioso de la FreeBSD es que cuando se activa la opcion de firewalling, el nucleo, por defecto, pilla el file por defecto de /etc que normalmente filtra todos los paquetes de todos los dispositivos y no deja pasar absolutamente nada por ningun lado. NO como en linux. Por lo que nos toca dar un paso intermedio. Dos opciones pues. La primera es modificando la configuracion script del firewall. Un ejemplo viene a continuacion.

En el fichero /etc/rc.conf tenemos que añadir lo siguiente:

```
gateway_enable=''YES''
firewall_enable=''YES''
firewall_script=''/etc/firewall/fwrules''
```

La primera linea ya la habiamos puesto anteriormente. En las otras dos, la primera nos permite trabajar con ipfw (ipchains en linux) y la segunda nos permite pasarle las rules al ipfw desde un file (ipchains-restore en linux)

Una vez añadidas estas lineas creamos directorio en /etc llamado 'firewall':

```
mkdir /etc/firewall
```

y creamos alli el fichero 'fwrules' que va a contener:

```
--- CUT ----
# Firewall rules
# QuasaR of UNDERSEC Security Team
# Gracias a Marc Silver (marcs@draenor.org)
# Definimos un alias sobre el que trabajar
fwcmd=''/sbin/ipfw''
# Borramos las rules que podamos tener establecidas de antemano.Ñunca se
# sabe y asiños ahorramos un huevo de problemas.
$fwcmd -f flush
# Y ahora voy a piñon, lo dejo pasar absolutamente todo
$fwcmd add allow ip from any to any via lo0
$fwcmd add allow ip from any to any via ed0
$fwcmd add allow ip from any to any via ppp0
--- EOF ----
```

Si, ya se que he dejado pasar todo. Pero es que no me quiero enrollar ahora explicando rules y tal. Que cada uno se lo haga a medida. La segunda opcion es mas rapida y posiblemente practica, pero menos segura. Hay que recompilar el kernel con la opcion:

```
options IPFIREWALL_DEFAULT_TO_ACCEPT
```

Ahora ya podemos ejecutar el pppd al serial. Funciona exactamente igual que en linux. Por lo que la opcion seria (mas info ver seccion linux):

```
pppd /dev/pilot 57600 :ipdepalm local crtscts passive proxyarpñoauth
```

Y con esto, la palm deberia de funcionar perfectamente. Salvo follones con las rutas estaticas del route. Estad atentos. Pero ya digo que deberia de funcionar. Solo le hace falta el connect de la palm para que se conecte.

4 CURIOSIDADES

Una vez conectada la palm al ordenador, en plataformas windows no permite encontrar la palm como un dispositivo a parte del propio windows. Sin embargo , no ocurre igual desde el resto de plataformas. En el resto de plataformas (entiendase Linux y FreeBSD) al asignarle una ip e incluso una direccion MAC a la palm, esta se considera como un dispositivo aparte, puediendose acceder a traves de la ip. Esto nos permite usar scaneos, pings, traceroutes y cualquier otra utilidad de red contra la palm. Y es entonces cuando nos encontramos con las cosas mas curiosas. Es divertido ver como un traceroute desde la RH pasa por la FreeBSD y llega hasta la palm. O el camino contrario, Ver como la palm accede al IRC desde la FREEBSD pasando por NAT por la RH. Ejemplillo?:

NOTESE que estoy desde quasar (RH) pasa por nekroid (FreeBSD)
y llega a INET.

```
[root@quasar ~]# traceroute palm
traceroute to palm.undersec.org (192.168.2.5), 30 hops max, 38 byte packets
1 ñekroid (192.168.2.4)  2.212 ms  1.129 ms  1.233 ms
2  palm (192.168.2.5)  35.443 ms  36.549 ms  34.745 ms
[root@quasar ~]#
```

Mas cosillas. La palm es ahora un terminal en la red y claro, soporta tcp. MMMMMmm... sera nukeable?. Correcto si. Cualquier nuke con igmps o flood deja la palm completamente tostada!. La pila TCP/IP no es ninguna maravilla y claro sale a relucir. De hecho, hasta un scanneo de fingerprints del nmap la deja tostada. Hablando de tostamientos, recomiendo la utilidad crash.prc que detecta un crashy resetea la palm en caliente por ti, sin darle la vuelta y darle al boton de reset. Busquese la susodicha utilidad en http://www.palmgear.com por ese mismo nombre.

Podria seguir explicando cosillas, como lo de las passwords vulnerables en el backup de la palm en el file Unsaved_Preferences.prc pero casi que esto es otra historia.... ;)

5 CONCLUSIONES

El bichito llamado palm es una maravilla y eternamente flexible aunque debe quedar claro que esta concebida como agenda personal y nunca hay que olvidar esa idea.

Las pruebas han dado siempre resultado positivo. Se realizaron con los los elementos indicados a continuacion:

Palm V - Palm OS 3.3

FreeBSD 4.0 STABLE

Linux Debian 2.2.17

6 AGRADECIMIENTOS Y SALUDOS

1. Pues tengo que agradecer eternamente aquellas primeras pruebas que se hicieron en la benagua party con el superportatil a Pope. Tengo que agradecer casi el resto de las pruebas sobre Linux a Sp4rk y su Debian chunga cuando la Hackmeeting.
2. Tengo que agradecer a mi madre que me diera pelas para poder ir a los sitios anteriores y poder haber hecho las pruebas.
3. Y tengo que agradecer a personas mas indirectas el dar animos cuando estas en momentos de bajon y sin ganas de hacer nada... Neko^_^ , Raise :*

Y ahora los saludos: UNDERSEC :* (http://www.undersec.com) & Netsearch (http://www.netsearch-ezine.com) ..... guarris!

7 DESPEDIDA

Espero que el articulo sirva a muchas personas y contribuya para que alguien no se tenga que dejar los cuernos mas....ya me los he dejado yo.

Para cualquier sugerencia o duda estoy en: quasar@netsearch-ezine.com
hasta que me vuele el correo.

Ta otra....