Hackin' LaFonera

a.k.a.

"How I did it"

by ***$iMol3$o***

1. Introduzione

Questo piccolo documento vuole essere una specie di report sulla mia personale esperienza nella sostituzione del software del social router La Fonera con una versione aperta del sistema operativo DD-WRT. La procedura qui esposta può essere liberamente scaricata dalla rete e assolutamente non vuole essere un documento esaustivo in merito a questo genere di procedure.

2. Disclaimer

Il progetto di social networking promosso da FON® è da lodare per la temerarietà dell'iniziativa e per i notevoli risultati raggiunti. Per questo motivo, questo documento non vuole assolutamente essere di incentivo al soverchiamento degli scopi del progetto, ma solo un documento sulle possibilità offerte dai mezzi trasmissivi a disposizione.
In pieno accordo con la filosofia Hacker dello "smontare per capire", tutto ciò che leggete è stato redatto al fine di aggiungere la mia personale esperienza al patrimonio di conoscenza collettiva realizzato tramite guide, manuali, howto e qualsiasi altro media volto alla condivisione dei saperi.
Gli autori di questo documento non si assumono alcuna responsabilità per l'applicazione di questa documentazione per fini che vadano oltre i paletti definiti da qualsiasi tipo di legge, regolamento, accordo (sia verbale che scritto).
I fruitori di queste informazioni sono quindi tacitamente consapevoli di assumersi le proprie responsabilità nei confronti di terzi detentori di qualsiasi diritto di proprietà e sfruttamento; in breve: **leggete a vostro rischio e pericolo**.

3. Hacking La Fonera: preparazione

Cosa vi serve per modificare la Fonera:

- Connessione a internet
- Una macchina Slackware 12.0 (:-D) con (almeno) una scheda Ethernet
- Un cavo cross per connettere la Fonera oppure un HUB/Switch su cui sia collegata la macchina Slack.
- Una macchina con scheda WiFi che supporti WPA.

4. Primo passo: Abilitare SSH

Per modificare il software dell'AP sarà necessario operare a step. Per prima cosa sarà necessario abilitare il servizio ssh sul software intonso della Fonera. In seguito sarà possibile accedere al social router attraverso il server ssh.
Sempre mantenendo LaFonera disconnessa dalla rete internet, effettuate una connessione alla rete WiFi con ESSID MyPlace sul canale 6 mantendo la vostra periferica WiFi in DHCP. Utilizzate come password WPA il serial number che trovate sull'etichetta sotto la Fonera, oppure sulla scatola della stessa.
Una volta connessi alla rete WiFi, nel vostro browser preferito collegatevi all'indirizzo 192.168.10.1, vi si presenterà l'interfaccia di configurazione del router.

ATTENZIONE

Nella sezione Status verificate che la versione del firmware sia la _0.7.1 r2_, questo howto può essere applicato solo con questa versione. Nell'eventualità che l'apparecchio abbia un firmware differente, resettatelo tramite l'apposito pulsante posto sotto l'AP e ripetete i passi si qui fatti.

Nella sezione advanced (autenticatevi tramite *admin/admin*) modificate le impostazioni nella scheda **Internet Connetion** scegliendo la modalità **Static IP** come segue:

```
IP 192.168.1.254
NM 255.255.255.0
GW 192.168.1.1
DNS 88.198.165.155
```

ed effettuate il submit e riavviate l'AP (scollegandolo e ricollegandolo alla rete elettrica).

ATTENZIONE

E' categoricamente importante sottolineare alcuni concetti:

1. Utilizzando l'indirizzo 192.168.1.254/24 sarà in seguito connettersi al medesimo indirizzo nella fase di flashing del firmware. Non è comunque indispensabile seguire pedestremente queste configurazioni, nel caso la vostra rete sia differente.
2. Sarà necessario accedere alla macchina Slackware (che nel mio caso è anche il gw) per l'upload del nuovo firmware, fate quindi in modo di poter raggiungere tale macchina direttamente.
3. Ultimo ma non per importanza, settate correttamente il DNS all'indirizzo indicato. Tramite questo indirizzo La Fonera accede ad un falso server degli aggiornamenti, il quale chiede all'AP di eseguire il demone SSH. Inserendo un diverso indirizzo per il DNS

Verificate la corretta configurazione dell'AP riconnetendovi secondo il metodo indicato.
Se tutto è andato a buon fine, potete ora collegare La Fonera con il cavo UTP alla rete internet e attendere qualche momento che la rete sia adeguatamente configurata.
Riavviate nuovamente il router.
Una volta ristabilita la connessione WiFi con MyPlace potrete effettuare un accesso via SSH a 192.168.10.1 tramite root/admin :-)

```
$ ssh root@192.168.10.1
root@192.168.10.1's password:


BusyBox v1.1.3 (2006.11.27-12:40+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.


 _______ _______ _______
|   ____||       ||   _   |
|   ____||   -   ||  |_|  |
|   |    |_______||__| |__|
|___|

 Fonera Firmware (Version 0.7.1 rev 2) -------------
  *
  * Based on OpenWrt - http://openwrt.org
  * Powered by FON - http://www.fon.com
 ----------------------------------------------------
root@OpenWrt:~#
```

Per finire, facciamo in modo che il servizio SSH rimanga attivo ed accessibile anche tramite la rete cablata. Dalla nostra connessione SSH rinominiamo lo script in modo che venga eseguito all'avvio:

```
root@OpenWrt:~# mv /etc/init.d/dropbear /etc/init.d/S50dropbear
```

E modifichiamo il firewall:

```
root@OpenWrt:~# vi /etc/firewall.user
```

decommentando le seguenti righe:

```
### Open port to WAN
## -- This allows port 22 to be answered by (dropbear on) the router
```

```
iptables -t nat -A prerouting_rule -i $WAN -p tcp --dport 22 -j ACCEPT
iptables        -A input_rule      -i $WAN -p tcp --dport 22 -j ACCEPT
```

Riavviamo quindi i servizi e iptables:

```
root@OpenWrt:~# /etc/init.d/S50dropbear
root@OpenWrt:~# /etc/firewall.user
```

Ora sarà possibile abbandonare la rete WiFi e rieffettuare l'accesso via rete cablata all'indirizzo 192.168.1.254 (o quello che avete configurato per la rete locale):

```
# ssh root@192.168.1.254
root@192.168.1.254's password:


BusyBox v1.1.3 (2006.11.27-12:40+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.


 _______ _______ _______
|   ____||       ||   _   |
|   ____||   -   ||  | |  |
|   |    |_______||__| |__|
|___|

 Fonera Firmware (Version 0.7.1 rev 2) -------------
  *
  * Based on OpenWrt - http://openwrt.org
  * Powered by FON - http://www.fon.com
 ----------------------------------------------------
root@OpenWrt:~#
```

Infine, dalla console sulla Fonera modifichiamo lo script che cercherà nuovamente di chiudere le connessioni dalla rete locale.

```
root@OpenWrt:~# vi /bin/thinclient
```

Modifichiamo l'ultima riga del file /bin/thinclient in modo che appaia così:

```
#. /tmp/.thinclient.sh
cp /tmp/.thinclient.sh /tmp/thinclient-$(date '+%Y%m%d-%H%M')
```

A questo punto chiudiamo la connessione SSH e riavviamo il router.

5. Il nuovo firmware

Accediamo nuovamente alla Fonera via ssh e scarichiamo nella directory **/tmp** un nuovo kernel di openwrt:

```
root@OpenWrt:~# cd /tmp/
```

E scarichiamo il nuovo kernel:

```
root@OpenWrt:~# wget http://Fonera.info/camicia/openwrt-ar531x-2.4-vmlinux-
CAMICIA.lzma
Connecting to Fonera.info[62.81.199.144]:80
openwrt-ar531x-2.4-v 100% |
*******************************************************************************
********|   512 KB    00:00 ETA
root@OpenWrt:~#
```

In seguito carichiamo il nuovo firmware come segue:

```
root@OpenWrt:~# mtd -e vmlinux.bin.l7 write openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma
vmlinux.bin.l7
Unlocking vmlinux.bin.l7 ...
Erasing vmlinux.bin.l7 ...
```

```
Writing from openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma to vmlinux.bin.l7 ...  [w]
root@OpenWrt:~#
```

State tranquilli, ci vorranno alcuni minuti. In seguito riavviamo il router:

```
root@OpenWrt:~# reboot && exit
Connection to 192.168.1.254 closed.
```

Riconnettiamoci appena possibile e procediamo con la seconda parte del flash. Nuovamente scarichiamo un file in **/tmp**:

```
root@OpenWrt:~# wget http://Fonera.info/camicia/out.hex
Connecting to Fonera.info[62.81.199.144]:80
out.hex              100% |
*******************************************************************************
********|  4096       00:00 ETA
root@OpenWrt:~#
```

E provvediamo a caricarlo tramite mtd:

```
root@OpenWrt:~# mtd -e "RedBoot config" write out.hex "RedBoot config"
Unlocking RedBoot config ...
Erasing RedBoot config ...
Writing from out.hex to RedBoot config ...  [w]
root@OpenWrt:~#
```

In questo modo abbiamo sovrascritto la configurazione di RedBoot: questa condizione porterà LaFonera a non trovare più il kernel del sistema operativo, per cui il boot si interromperà e non sarà possibile accedere al router se non tramite telnet verso l'IP 192.168.1.254 (indipendentemente dal fatto che abbiate configurato questo indirizzo o meno prima) e la porta 9000.

La parte semplice dell'howto è finita :-). Ora dobbiamo procedere a configurare il server TFTP.

6. Il server TFTP su Slacware 12

Scaricate e installate il pacchetto tftp da *ftp://ftp.slackware.com/pub/slackware/slackware-12.0/slackware/n/tftp-hpa-0.48-i486-1.tgz*

e create la cartella **/tftpboot/**

Quindi modificate **/etc/inetd.conf** per abilitare il **tftp** server decommentando la linea corretta, come segue:

```
# Tftp service is provided primarily for booting.  Most sites
# run this only on machines acting as "boot servers."
 tftp  dgram   udp     wait    root    /usr/sbin/in.tftpd  in.tftpd -s /tftpboot -r
blksize
```

Infine riavviate inetd:

```
# /etc/rc.d/rc.inetd restart
Starting Internet super-server daemon:  /usr/sbin/inetd
```

7. DD-WRT: il firmware

Collegandovi a *http://www.dd-wrt.com/dd-wrtv3/dd-wrt/downloads.html* potrete scaricare il software necessario per il flash della Fonera. Si tratta di una versione BETA, inolte dovrete partire dal link evidenziato per spostarvi in:
-> beta/ -> FONERA/ -> 2007 - 200721/

Effettuate il download dei file root.fs e vmlinux.bin.l7 in **/tftpboot/**

```
# ls /tftpboot/
root.fs  vmlinux.bin.l7
```

ATTENZIONE
Purtroppo la versione 2007 - 0803 non sembra funzionare, sarà in seguito possibile aggiornare il firmware direttamente da DD-WRT.

Ora siamo pronti. Scolleghiamo la presa di corrente della Fonera e prepariamoci alla connessione telnet.

8. DD-WRT: Telnet

Dalla documentazione disponibile sembra sia possibile effettuare la connessione telnet entro i primi 10 secondi di uptime della Fonera. Effettuate la connessione date un INVIO per vedere il Prompt di RedBoot:

```
# telnet 192.168.1.254 9000
Trying 192.168.1.254...
Connected to 192.168.1.254.
Escape character is '^]'.

/home/alfa/Atheros_Beta5.0/linuxsrc/src/redboot_fon1/ecos/packages/devs/eth/mips/ar
531x/current/src/ae531xecos.c#390:ae531x_send AHB ERROR: AR531X_DEBUG_ERROR =
00000001
/home/alfa/Atheros_Beta5.0/linuxsrc/src/redboot_fon1/ecos/packages/devs/eth/mips/ar
531x/current/src/ae531xecos.c#393:ae531x_send AHB ERROR status_4 = 00000555
RedBoot>
```

Ignorate gli errori :-) e configuriamo la rete in modo tale da dare come default server il nostro server TFTP Slackware 12 (che ha indirizzo 192.168.1.1):

```
RedBoot> ip_address -l 192.168.1.254/24 -h 192.168.1.1
/home/alfa/Atheros_Beta5.0/linuxsrc/src/redboot_fon1/ecos/packages/devs/eth/mips/ar
531x/current/src/ae531xecos.c#390:ae531x_send AHB ERROR: AR531X_DEBUG_ERROR =
00000001
/home/alfa/Atheros_Beta5.0/linuxsrc/src/redboot_fon1/ecos/packages/devs/eth/mips/ar
531x/current/src/ae531xecos.c#393:ae531x_send AHB ERROR status_4 = 00000145
IP: 192.168.1.254/255.255.255.0, Gateway: 0.0.0.0
Default server: 192.168.1.1
```

Inizializiamo il firmware:

```
RedBoot> fis init
/home/alfa/Atheros_Beta5.0/linuxsrc/src/redboot_fon1/ecos/packages/devs/eth/mips/ar
531x/current/src/ae531xecos.c#390:ae531x_send AHB ERROR: AR531X_DEBUG_ERROR =
00000145
/home/alfa/Atheros_Beta5.0/linuxsrc/src/redboot_fon1/ecos/packages/devs/eth/mips/ar
531x/current/src/ae531xecos.c#393:ae531x_send AHB ERROR status_4 = 00000145
About to initialize [format] FLASH image system - continue (y/n)? y
*** Initialize FLASH Image System
... Erase from 0xa87e0000-0xa87f0000: .
... Program from 0x80ff0000-0x81000000 at 0xa87e0000: .
RedBoot>
```

E infine facciamo l'upload dal server TFTP il root.fs precedentemente scaricato:

```
RedBoot> load -r -v -b 0x80041000 root.fs
/home/alfa/Atheros_Beta5.0/linuxsrc/src/redboot_fon1/ecos/packages/devs/eth/mips/ar
531x/current/src/ae531xecos.c#390:ae531x_send AHB ERROR: AR531X_DEBUG_ERROR =
00000001
/home/alfa/Atheros_Beta5.0/linuxsrc/src/redboot_fon1/ecos/packages/devs/eth/mips/ar
531x/current/src/ae531xecos.c#393:ae531x_send AHB ERROR status_4 = 00000145
Using default protocol (TFTP)
\
Raw file loaded 0x80041000-0x802e5fff, assumed entry at 0x80041000
RedBoot>
```

Se tutto sarà configurato a dovere il file verrà allocato sull'AP. Procediamo

quindi a flasharlo:

```
RedBoot> fis create -b 0x80041000 -f 0xA8030000 -l 0x002C0000 -e 0x00000000 rootfs
/home/alfa/Atheros_Beta5.0/linuxsrc/src/redboot_fon1/ecos/packages/devs/eth/mips/ar
531x/current/src/ae531xecos.c#393:ae531x_send AHB ERROR status_4 = 00000145
... Erase from 0xa8030000-0xa82f0000: ..........................................
... Program from 0x80041000-0x80301000 at
0xa8030000: ........................................
... Erase from 0xa87e0000-0xa87f0000: .
... Program from 0x80ff0000-0x81000000 at 0xa87e0000: .
RedBoot>
```

Facciamo l'upload dal server TFTP del nuovo kernel:

```
RedBoot> load -r -v -b 0x80041000 vmlinux.bin.l7
Using default protocol (TFTP)
-
Raw file loaded 0x80041000-0x80100fff, assumed entry at 0x80041000
RedBoot>
```

E provvediamo a caricarlo sulla eprom:

```
RedBoot> fis create -r 0x80041000 -e 0x80041000 -l 0x000E0000 vmlinux.bin.l7
/home/alfa/Atheros_Beta5.0/linuxsrc/src/redboot_fon1/ecos/packages/devs/eth/mips/ar
531x/current/src/ae531xecos.c#390:ae531x_send AHB ERROR: AR531X_DEBUG_ERROR =
00000001
/home/alfa/Atheros_Beta5.0/linuxsrc/src/redboot_fon1/ecos/packages/devs/eth/mips/ar
531x/current/src/ae531xecos.c#393:ae531x_send AHB ERROR status_4 = 00000145
... Erase from 0xa82f0000-0xa83d0000: ..............
... Program from 0x80041000-0x80101000 at 0xa82f0000: ............
... Erase from 0xa87e0000-0xa87f0000: .
... Program from 0x80ff0000-0x81000000 at 0xa87e0000: .
RedBoot>
```

Finalizziamo l'installazione con l'ultimo fis:

```
RedBoot> fis create -f 0xA83D0000 -l 0x00010000 -n nvram
/home/alfa/Atheros_Beta5.0/linuxsrc/src/redboot_fon1/ecos/packages/devs/eth/mips/ar
531x/current/src/ae531xecos.c#390:ae531x_send AHB ERROR: AR531X_DEBUG_ERROR =
00000001
/home/alfa/Atheros_Beta5.0/linuxsrc/src/redboot_fon1/ecos/packages/devs/eth/mips/ar
531x/current/src/ae531xecos.c#393:ae531x_send AHB ERROR status_4 = 00000145
... Erase from 0xa87e0000-0xa87f0000: .
... Program from 0x80ff0000-0x81000000 at 0xa87e0000: .
RedBoot>
```

Infine riavviate il router con un bel:

```
RedBoot> reset
```

e preparatevi al divertimento.

9. Conclusione

Al riavvio il vostro nuovo Accesso Point sarà raggiungibile via web tramite l'indirizzo 192.168.1.1. Potete collegarvi alla sezione amministrazione tramite *root/admin* e configurare tutto il necessario.

10. Riferimenti

- Abilitazione SSH: **http://stefans.datenbruch.de/laFonera/#kolofonium**
- Flashare il firmware: **http://dltv.files.wordpress.com/2007/03/laFonera.pdf**
- Altra guida completa: **http://dltv.wordpress.com/off-the-wall/a-guide-to-hacking-the-la-Fonera-wireless-router/**