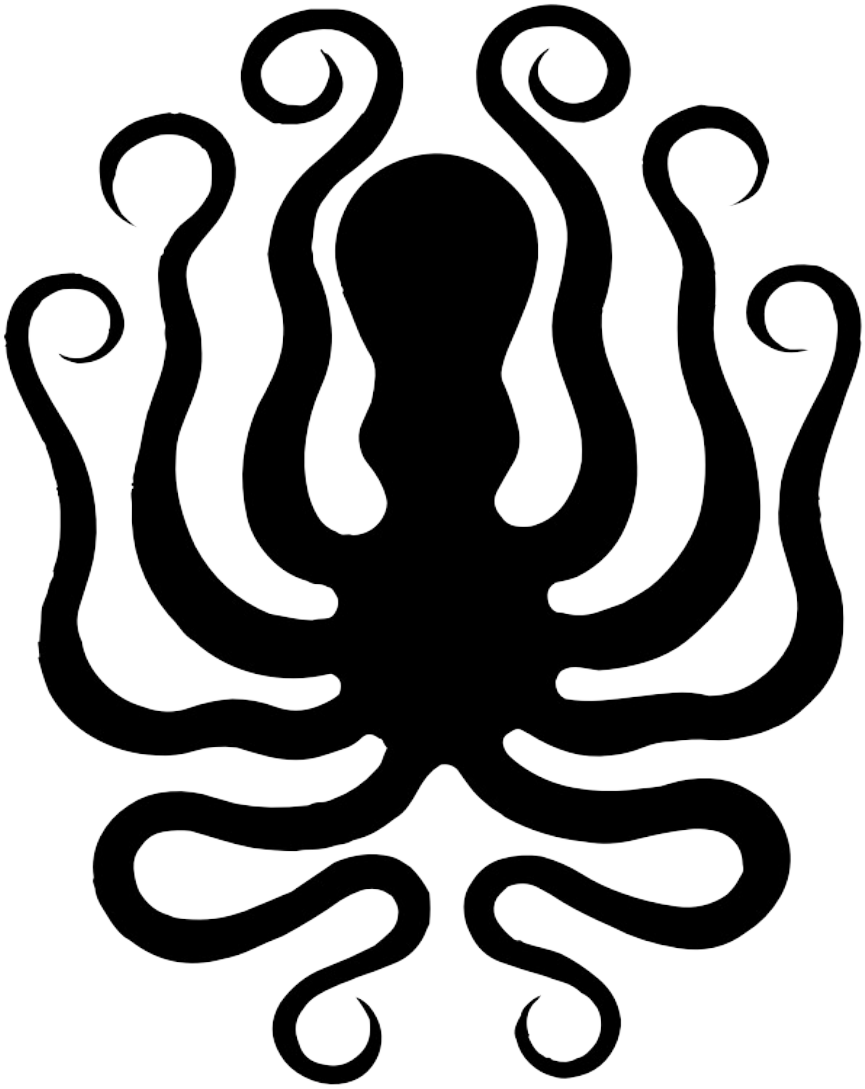

Hacking
“La Fonera” con Firmware DD-WRT

By
Mattioli Brando

Premessa

Da un paio di anni, nel mio armadio, stava rinchiusa la Fonera. Un router molto elegante e compatto che veniva distribuito gratuitamente o per pochissimi Euro con lo scopo di promuovere il "Movimento Fon". (Per maggiori Informazioni, Clicca Qui!)

Navigando in Internet, sono poi venuto a conoscenza che era possibile rimuovere il firmware nativo della Fonera (firmware molto restrittivo) e sostituirlo con un'altro, ovvero il DD-WRT. Per poter fare questa modifica, occorrevano però una serie di Applicazioni, editare qualche riga di codice, e tanta tanta pazienza. Di guide, ne ho viste tantissime, con vari metodi, ma molte erano incomplete, altre erano molto sintetiche e non sempre chiare o magari era tutto comprensibile, ma nel momento in cui si dovevano utilizzare le applicazioni segnalate qualcuna mancava o non era più disponibile. Alla fine spulciando a destra e manca, archiviando un po' di applicazioni e sommando qualche guida, sono riuscito nel mio intento, ovvero: cancellare il firmware della Fonera e sostituirlo con DD-WRT.

Ho deciso quindi di creare questa nuova guida e renderla pubblica assieme a tutte le altre, sperando che possa rivelarsi utile ad altri che come me si mettono alla ricerca di un "How To" chiaro e completo per sbloccare la Fonera.

ATTENZIONE Questa guida è da considerarsi a solo scopo Informativo ed Educativo, perciò io non mi ritengo responsabile di un utilizzo errato che ne potrebbe essere tratto; né tantomeno nel caso in cui la Fonera andasse in crash. Ricordiamoci che la modifica del Firmware, è sempre un operazione molto delicata.

Preparazione

Per poter procedere con la modifica del Firmware, occorre scaricare una serie di Applicazioni che potrete trovare in Google, oppure scaricando direttamente il pacchetto completo da Qui! In questo pacchetto infatti, troverete tutte le applicazioni che vedete qui sotto elencate, per evitarvi perdite di tempo nel ricercarle in internet.

Applicazioni:

- ✔ Putty
- ✔ root.fs
- ✔ vmlinux.bin.l7
- ✔ Hfs
- ✔ Tftp Server
- ✔ Particolare Pagina HTML per Abilitare l'SSH
- ✔ out.hex
- ✔ openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma

Identificazione Firmware

Per prima cosa, bisogna scoprire il firmware della nostra Fonera, poiché in base a quello dovremo abilitare l'SSH. Considerate che le Fonere recenti hanno la versione del firmware 0.7.1 r3 o superiore, mentre quelle vecchie teoricamente dovrebbero avere la versione 0.7.1 r1. Per poter verificare la versione del firmware, dobbiamo:

- Disattivare tutti i Firewall (compreso quello di Windows)
- Collegare con il cavo in dotazione (rj45) la nostra Fonera alla porta Ethernet del nostro PC
- Settare la nostra Scheda di Rete, con i seguenti Valori:
  IP: 169.254.255.2
  Subnet: 255.255.0.0
  Default Gateway: 169.254.255.1
  DNS: 169.254.255.1

Ora, accendiamo la nostra Fonera e attendiamo che tutti e 3 i Leds siano attivi. Apriamo il browser e digitiamo il seguente indirizzo:

http://169.254.255.1

Username: **root**
Password: **admin**

Entreremo quindi nel Pannello di Controllo della Fonera. Clicchiamo su Status e visioniamo la versione del firmware. Se la versione è la 0.7.1 r1, passiamo direttamente nella Sezione "Abilitazione SSH", se invece la versione del firmware è la 0.7.1 r2 o la 0.7.1 r3 (come nel mio caso), dovremo eseguire la procedura di downgrade del firmware. In poche parole riporteremo la versione del firmware alla 0.7.1 r1.

Downgrade Firmware

Per poter "downgradare" il firmware della Fonera, alla versione a noi interessata, occorre seguire una procedura di reset. Prendiamo la nostra Fonera e:

- Procuriamoci uno stuzzicadente o un oggetto con una punta molto fine e infiliamolo nel foro del reset (il foro si trova sotto la Fonera).
- Tenete premuto il bottone del reset per 30 secondi.
- Tenendo sempre premuto il bottone del reset, passati i 30 secondi, staccate l'alimentazione della Fonera.
- Sempre tenendo premuto il bottone, rimettete l'alimentazione.
- Attendete finchè il Led "W-LAN" appare e subito dopo sparisce (Circa un paio di minuti; 2 o 3 minuti di pressione dello stuzzicadente)
- Nel momento in cui il Led "W-LAN" appare e poi sparisce, smettiamo di pressare il bottone di reset e attendiamo altri 2 o 3 minuti, fino a quando il Led "W-LAN" riappare.
- Ora ricolleghiamoci al Pannello di Controllo e se andiamo a visionare la versione del firmware, magicamente sarà la 0.7.1 r1. Ora possiamo procedere con l'abilitazione dell'SSH

Abilitazione SSH

Per abilitare l'SSH, basterà andare nel pacchetto che vi ho fatto scaricare e cercare il file sshenable.htm (è probabile che sia compresso in un file .rar – decomprimetelo).
Una volta trovato il file, apritelo con il vostro browser e cliccate sul bottone "Submit"

Abilitazione RedBoot

Avviamo HFS (applicazione che trovate nel pacchetto). La prima volta che eseguiamo HFS, ci chiederà se vogliamo includere HFS nel nostro menù contestuale. Scegliamo "No".
Successivamente clicchiamo con il tasto destro nell'icona della casa e selezioniamo "Add Files" e aggiungiamo i file:

- openwrt-ar531x2.4-vmlinux-CAMICIA.lzma
- out.hex

Lasciamo attivo HFS - non chiudiamolo - e apriamo Putty (anche questa applicazione, la trovate nel pacchetto). Selezionate come protocollo l'SSH e ci colleghiamo in SSH alla Fonera

inserendo l'IP:

169.254.255.1

e clicchiamo su "Open". Se questa è la prima volta che ci colleghiamo alla Fonera in SSH, ci verrà richiesto di salvare la chiave SSH con un prompt. Accettiamo (Yes).
Ci verranno richiesti i dati di autenticazione e noi digitiamo:

Username: **root**
Password: **admin**

Premiamo su Invio. Ora siamo entrati nella Fonera. Adesso dovremo eseguire alcuni command. Copiate uno per volta ogni comando che vedete qui, e incollatelo nell'applicazione e successivamente cliccate su Invio.

mv /etc/init.d/dropbear /etc/init.d/S50dropbear

vi /etc/firewall.user

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

#. /tmp/.thinclient.sh

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

cd /tmp

wget http://169.254.255.2/openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma

Mi raccomando, ogni linea di codice che vedete qui sopra riportata, dovrete copiarla esattamente uguale, incollarla in putty e successivamente confermare con Invio. Con l'ultima stringa di codice che avete qui sopra, dovrete attendere che il trasferimento termini. Successivamente, potrete lanciare i seguenti comandi e attendere che il prompt ritorni:

mtd -e vmlinux.bin.l7 write openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma vmlinux.bin.l7

reboot

Effettuato il reboot, attendiamo 2-3 minuti fino a quando tutti e 3 i Leds lampeggiano.
Apriamo nuovamente Putty per ricollegarci in SSH

Username: **root**
Password: **admin**

Eseguiamo i seguenti comandi e attendiamo, anche in questo caso, che ci ritorni il prompt dei comandi.

cd /tmp

wget http://169.254.255.2/out.hex

mtd -e "RedBoot config" write out.hex "RedBoot config"

reboot

Ottimo! Ora è abilitato il RedBoot che permette di accedere al bootloader. Questo ci permetterà di flashare la nostra Fonera con il firmware DD-WRT. Chiudiamo HFS.

Flasshing DD-WRT

Per prima cosa, dovremo cambiare l'IP e la Subnetmask della nostra scheda di rete, mentre lasciamo inalterati Gateway e DNS.

IP: 192.168.1.166
Subnet 255.255.255.0

Apriamo il programma TFTP32 (che trovate nel pacchetto che avete scaricato). Controlliamo che nella cartella da dove lanciamo TFTP32, ci siano anche i files:

- root.fs
- vmlinux.bin.l7

Apriamo Putty e selezioniamo come protocollo Telnet e come IP 192.168.1.254 e come porta la 9000. Stacchiamo l'alimentazione alla Fonera e in una finestra di DOS digitiamo:

ping 192.168.1.254 -t

e poi digitiamo Invio. Mantenendo aperta la finestra DOS, ricolleghiamo l'alimentazione alla Fonera e nel momento in cui la Fonera, risponde al nostro Ping (che visualizzerete nella finestra di DOS) lanciate Putty, con le impostazione elencate qui sopra. Questo ci permette di essere connessi in RedBoot. Mantenendo sempre attivo TFTP32, eseguiamo i seguenti comandi (il comando fis richiede molto tempo, quindi non preoccupatevi, occorre solo un po' di pazienza. Generalmente richiede 10 minuti per comando. Voi digitate il nuovo, solo quando vi ritornerà il prompt):

ip_address -l 192.168.1.254/24 -h 192.168.1.166

fis init

Premiamo “Y”, e confermiamo sempre con Enter (Invio).

load -r -v -b 0x80041000 root.fs

fis create -b 0x80041000 -f 0xA8030000 -l 0x002C0000 -e 0x00000000 rootfs

load -r -v -b 0x80041000 vmlinux.bin.l7

fis create -r 0x80041000 -e 0x80041000 -l 0x000E0000 vmlinux.bin.l7

fis create -f 0xA83D0000 -l 0x00010000 -n nvram

reset

Dopo il reset avremo finalmente la DD-WRT sulla nostra Fonera! Ora, per poterci collegare al Nuovo Pannello di Controllo dovremo cambiare nuovamente le opzioni della nostra scheda di rete in:

IP: 169.254.255.2
Subnet: 255.255.0.0
Default Gateway: 169.254.255.1
DNS: 169.254.255.1

Aprire il browser e digitare:

http://192.168.1.1

Username: **root**
Password: **admin**

E il gioco è fatto! ;-)