Atheros drivers installation

Στην ενότητα αυτή θα δούμε πως μπορείτε να εγκαταστήσετε τους κατάλληλους οδηγούς στο linux έτσι ώστε να μπορείτε να χρησιμοποιήσετε τη λειτουργία injection με την atheros κάρτα σας. Όλες οι διανομές συμπεριλαμβάνουν στον πυρήνα τους τα απαραίτητα drivers για τη λειτουργία της atheros κάρτας σας, ωστόσο αν θέλετε να χρησιμοποιήσετε το injection θα πρέπει να ακολουθήσετε τα παρακάτω βήματα. Υπάρχουν δύο ειδών drivers οι mac80211 και οι ieee80211 (ή net80211). Οι mac80211 έχουν αρχίσει και αντικαθιστούν τους ieee802.11και συμπεριλαμβάνονται στον πυρήνα Linux από την έκδοση 2.6.25. Ωστόσο, δεν είναι ακόμη ώριμοι κι έτσι προτείνεται η χρήση των ieee80211 και με αυτούς θα ασχοληθούμε στη συνέχεια.

Προετοιμασία

Για να κάνετε compile τους drivers θα χρειαστείτε τα ακόλουθα:

- Τις επικεφαλίδες του πυρήνα Linux που χρησιμοποιείται. Για να τις κατεβάσετε στο Debian εκτελέστε:

```
$ apt-get install linux-headers-$(uname –r)
```

- Το πακέτο build essential:

```
$ apt-get install build-essential
```

- Την έκδοση του gcc με την οποία μεταγλωττίστηκε ο πυρήνας σας. Θα πρέπει να προσέξετε να ταιριάζουν τα δύο πρώτα νούμερα για παράδειγμα μπορείτε να χρησιμοποιήσετε το gcc-**3.4.**6 για έναν πυρήνα που μεταγλωττίστηκε με το gcc-**3.4.**1. Για πυρήνα 2.6.26 κατεβάστε το gcc-3.4:

```
$ apt-get install gcc-3.4
```

- Το πακέτο sharutils:

```
$ apt-get install sharutils
```

Blacklisting mac80211 driver version

Σε αυτό το βήμα θα ενημερώσουμε τον πυρήνα ώστε να μην φορτώνει το ενσωματωμένο driver mac80211 που διαθέτει. Στο σημείο αυτό θα πρέπει να δώσετε ιδιαίτερη προσοχή για να δουλέψει σωστά ο νέος driver που θα εγκαταστήσετε. Υπάρχουν δύο εκδόσεις του mac80211 για το atheros τσιπάκι, η ath5k και η ath9k. Για να δείτε ποια από τις δύο εκδόσεις διαθέτεται μεταβείτε στο φάκελο /lib/modules/$(uname -r)/kernel/drivers/net/wireless/ και ψάξτε για κατάλογο με

όνομα ath5k ή ath9k. Αν υπάρχουν και τα δύο έχετε και τους δύο drivers ενσωματωμένους. Ένας άλλος τρόπος είναι να ψάξετε για τα αρχεία ath5k.ko ή ath9k.ko. Η ύπαρξη κάποιου από τα δύο αρχεία σημαίνει και την ύπαρξη του αντίστοιχου driver.

Υπάρχουν δύο τρόποι για να κάνουμε black list τους ενσωματωμένους drivers:

- Αν υπάρχει το αρχείο

  /lib/modules/$(uname -r)/kernel/drivers/net/wireless/ath5k/ath5k.ko θα πρέπει να το μεταφέρετε σε ένα άλλο directory ομοίως και για το αρχείο /lib/modules/$(uname -r)/kernel/drivers/net/wireless/ath9k/ath9k.ko . Αφού το μετακινήσετε εκτελέστε:

```
$ depmod -ae
```

- Ανοίξτε το /etc/modprobe.d/blacklist με έναν editor και εισάγεται το

```
blacklist ath5k
```

σε μία νέα γραμμή. Ομοίως και για το ath9k αν υπάρχει στο σύστημά σας. Όποιον δρόμο και να ακολουθήσετε πρέπει να κάνετε επανεκκίνηση στο σύστημά σας πριν συνεχίσετε στα επόμενα βήματα.

Κατεβάστε και κάντε compile τον νέο driver

Στη συνέχεια θα κατεβάσουμε τους drivers και αφού τους κάνουμε patch ώστε να υποστηρίξουν το injection θα τους κάνουμε conpile και θα τους εισάγουμε στον πυρήνα. Θα χρησιμοποιήσουμε τους madwifi-ng οδηγούς και συγκεκριμένα την έκδοση rev3925 στην οποία είναι διαπιστωμένο ότι το injection λειτουργεί καλά:

```
$ svn -r 3925 checkout http://svn.madwifi-project.org/madwifi/trunk/ madwifi-ng
$ cd madwifi-ng
$ wget http://patches.aircrack-ng.org/madwifi-ng-r3925.patch
$ patch -N -p 0 -i madwifi-ng-r3925.patch
$ ./scripts/madwifi-unload
$ make
$ make install
$ depmod -ae
$ modprobe ath_pci
```

Εάν θέλετε μπορείτε να εγκαταστήσετε και νεότερη έκδοση του madwifi-ng. Για να βρείτε το κατάλληλο patch ανατρέξτε εδώ

Σημείωση

Αν δεν έχετε εγκατεστημένο το πακέτο subversion και η εντολή svn αποτύχει, μπορείτε να το κατεβάσετε και να το εγκαταστήσετε εκτελώντας:

```
$ apt-get install subversion

$apt-get install libapache2-svn
```