Nomadic Communications Labs

Alessandro Villani
avillani@science.unitn.it

Analysis of 802.11 Packets

BackTrack

- We will use a Linux Live distribution for this lab: BackTrack
  - http://www.remote-exploit.org/backtrack.html
- It has all the tools we need for wireless sniffing and monitoring, and we don't need to install any program on the laptop or ask for root passwd

BackTrack: Startup

- Boot from cd
- Login as root:
  - Login: `root`
  - Passwd: `toor`
- Start the graphics mode:
  - `startx`

BackTrack: iwconfig

- To get the Wireless Network Card parameters:
  - `iwconfig`
- The result is something like:

```
eth0      IEEE 802.11b  ESSID:“science-wifi"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 00:40:96:5E:0D:64
          Bit Rate:11 Mb/s   Tx-Power=20 dBm   Sensitivity=8/0
          Retry limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=46/100  Signal level=-73 dBm  Noise level=-88 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:34   Missed beacon:0
```

BackTrack: iwconfig

- To put the wireless Network Card in monitor mode (listening the channel 7):
  - `iwconfig eth0 mode monitor channel 7`
- If we give the iwconfig command again, the result is something like:

```
eth0      unassociated  ESSID:off/any
  Mode:Monitor  Frequency=2.442 GHz  Access Point: Not-Associated
  Bit Rate:0 kb/s   Tx-Power=20 dBm   Sensitivity=8/0
  Retry limit:7   RTS thr:off   Fragment thr:off
  Encryption key:off
  Power Management:off
  Link Quality:0  Signal level:0  Noise level:0
  Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
  Tx excessive retries:0  Invalid misc:51   Missed beacon:0
```

BackTrack: the task (suggestion)

- Run wireshark and start to acquire data from the wireless interface
- Try to get authentication and association between station and AP
- Try to correlate your 802.11 authentication with Radius MAC authentication, using ethereal on the server laptop

BackTrack: the task (suggestion)

- Explore some particular configuration:
  - MAC not registered in the radius server
  - Put as required a speed on a CISCO AP and configure a client so that it can not support that speed
- Verify if the packets acquired reflect what we expect from an 802.11 network!
- Play with fragmentation on AP and verify the packets sent and received by the clients

BackTrack: the task (suggestion)

- Use two laptop to acquire simultaneously the data on the same channel.
  Verify if the data acquired are the same and point out the difference, if any!
- Disable fragmentation, and use iperf with different packet sizes (for examples 800 and 2000) using tcp and udp in a bidirectional test. Acquire the data packets and describe them.

Lab Report

- You have to:
  - Describe the setup of the test
  - Describe the result obtained with schemes and examples (small dump of some significant packets)
  - Write down a short description of the data obtained and point out all the unexpected result you got!

Radius:

- To start the radius server:
  - `/etc/init.d/freeradius start`
- To add/remove the mac address authorized to connect to the wireless network, edit the file:
  - `/etc/freeradius/users`
- After any change to the radius configuration:
  - `/etc/init.d/freeradius reload`
- The accounting informations are stored in the directory:
  - `/var/log/freeradius/radacct`

Radius:

- The radius log is in the file /etc/freeradius/radius.log
  - If the MAC address of the Network Card is not in /etc/freeradius/users file:

```
Thu Mar 22 14:57:11 2007 : Auth: Login incorrect: [0015003c3b1a/0015003c3b1a]
   (from client AP1231 port 1259 cli 0015003c3b1a)
Thu Mar 22 14:57:14 2007 : Auth: Login incorrect: [0015003c3b1a/0015003c3b1a]
   (from client AP1231 port 1260 cli 0015003c3b1a)
Thu Mar 22 14:57:17 2007 : Auth: Login incorrect: [0015003c3b1a/0015003c3b1a]
   (from client AP1231 port 1261 cli 0015003c3b1a)
```

  - If the MAC address of the Network Card is in /etc/freeradius/users file:

```
Thu Mar 22 14:57:19 2007 : Auth: Login OK: [0015003c3b1a] (from client AP1231
   port 1262 cli 0015003c3b1a)
```