

# LAB 9: WiFi security – homework

# Homework

Based on captured sample data (same way as we did at the seminar) you should do offline dictionary attack and find the hidden password. The dictionaries and sample data is placed in IS.

To work out this homework you can choose tool whatever you want, but I recommend use Kali Linux. Use any file you can obtain from `/usr/share/wordlists/` (in Kali Linux, as you could see on the lecture).

- ▶ Live bootable ISO: <https://www.kali.org/downloads/>
- ▶ VMwareVirtualBox Image: <https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/>

Hint: you should use **one** of the “air\*-ng” family tools. It is recommended to read man pages of this tools before solving homework.

# Homework: report

**Deadline: 25th of April, 2017**

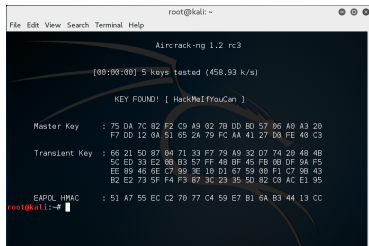
Format: **pdf file**

**Your report must contain:**

- ▶ Full command (with all options) which you use for solve this problem
- ▶ Screen-shot of used program with found WPA2 pass-phrase (see example bellow)

**Example:**

To solve this problem I used command "airtun-ng -a 00:14:22:56:F3:4E -t 0 -p captured.cap wlan0"



```
root@kali: ~  
File Edit View Search Terminal Help  
Aircrack-ng 1.2 rc3  
[00:00:00] 5 keys tested (458.93 k/s)  
KEY FOUND! [ HackMeIfYouCan ]  
Master Key : 75 DA 7C 82 F2 C9 A9 02 7B DD B0 57 06 A0 A3 20  
F7 DD 12 0A 51 65 2A 79 FC AA 41 27 D6 FE 48 C3  
Transient Key : 66 21 50 87 04 71 33 F7 79 A9 32 07 74 20 48 4B  
5C ED 33 E2 0B B3 57 FF 48 BF 45 FB 68 DF 94 F5  
EE 89 46 6E C7 99 3E 10 D1 67 59 00 F1 C7 56 43  
B2 E2 73 5F F4 F3 87 3C 23 35 50 82 C8 AC E1 95  
EAPOL HMAC : 51 A7 55 EC C2 70 77 C4 59 E7 B1 6A B3 44 13 CC  
root@kali:~#
```