

LAB 9: WiFi security – homework

On captures from

- ▶ offline dictionary attack and find the hidden password. Password was chosen from *rockyou* wordlist. SSID: *PA197-WPA-DICT2*
 - ▶ *rockyou* wordlist is downloaded to root user home directory on lab laptops
- ▶ offline brute-force attack based on story on next slide. SSID: *PA197-WPA-BF2*
- ▶ data analysis of decrypted capture of brute-force attacked network. SSID: *PA197-WPA-BF2*

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

Brute-Force attack

- ▶ Imagine scenario: You had few opportunities to sneak when user typed in password for wpa encrypted wireless network. Noticed few details which will help reduce number of possible combinations:
 - ▶ Password contains exactly 8 characters
 - ▶ first 2 characters are "ue"
 - ▶ third character is digit
 - ▶ fourth character was written with left hand and is lowercase
 - ▶ fifth character is space
 - ▶ rest of password are lowercase letters

- ▶ Client on SSID PA197-WPA-BF2 is downloading from AP every minute 1 text file using unsecured protocol
- ▶ Your task is to decrypt captured data with password from BF attack and find following:
 - ▶ filename
 - ▶ file content
 - ▶ protocol used for transport
 - ▶ user credentials

Hint: this can be done all with very popular network analyzer

Homework: report

Deadline: May 7, 2020 23:59

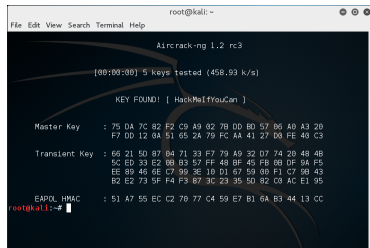
Format: **pdf file**

Your report must contain:

- ▶ Full command (with all options) which you use for solve assigned problems
- ▶ Screen-shots of used programs with found WPA2 pass-phrase (see example bellow)
- ▶ Data analysis

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 78 DD BD 57 86 48 A3 20  
F7 DD 12 0A 51 65 2A 79 FC AA 41 27 D8 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 08 B3 57 FF 48 BF 45 FB 86 DF 9A F5  
EE 89 46 6E D7 99 3E 10 D1 67 59 88 F1 C7 98 43  
B2 E2 73 5F F4 F3 87 3C 23 35 50 82 C3 AC E1 95  
EAPOL HMAC : 51 A7 55 EC C2 78 77 C4 59 E7 B1 6A B3 44 13 CC  
root@kali:~#
```