Please fill in the names with CAPITAL letters

Date	Name 1	Name 2	Name 3	Zaliczenie

WLAN Laboratory

Lab 11. Wireless 802.11 Security

Objective:

The students will learn about the 802.11 security mode. It will be show how can be sniff packets to obtain MAC addresses and how to crack a WEP key.

Student Prerequisites:

- knowledge of the basic WLAN configuration,
- familiarity with the self-learning material of the course,
- basic knowledge of the Linux OS and Windows,
- basic knowledge of IPv4 addresses

Hardware and Software to be used in this lab assignment:

PC with the wireless card (TPlink USB NIC) and os Linux (Ubuntu), aircrack-ng package, worked (configured) secured WLAN. (optional macchanger program).

Description of the Experiment:

During the exercise students sniff packets to obtain MAC addresses and crack a WEP key.

Lab Scenario:

Perform the attack on WEP secured WLAN. Take, decode WEP key and then log on to the targeted network. Attack the network “target-223” with secure 64 bit WEP key.

!!! See the tutorial at:

http://www.aircrack-ng.org/doku.php?id=simple_wep_crack

I)

Start the PC and identify wireless network adapters in PC (use: *ifconfig* and *iwconfig* commands, check the documentation eg. *man iwconfig*).
Write WLAN NIC name: ……………………………………………………………………….

Find what the networks work in your neighborhood, identify the WLAN network “target-223” which you will carry out the attack. (use: *sudo iwlist <NIC_name> scanning* command)
Write the “target-223” MAC address: .... and channel number: ....

II)

WLAN NIC standard working mode is **Managed** mode, in this mode the NIC cannot be use to capture WLAN packet. Prepare the WLAN adapter to work in network **monitor** mode.

Use *airmon-ng* command, check a command documentation (use: *man airmon-ng*). If command need a superuser permissions use *sudo* command eg. *sudo airnom-ng*. Expected results of *airmon-ng* are creation of a new virtual NIC interface working in monitor mode, static on selected channel (do not forget to specify WALN channel during the setup new NIC monitor interface). Check NICs and their working modes with *iwconfig* command. !NOTE If some other processes in Linux use your NIC at the same time it can injure capturing task, kill (use: *airmon-ng*) all injured process if necessary (check a command documentation use: *man airmon-ng*).

III)

Check out the parameters to run the sniffer packet (use: *man airodump-ng*).

Run the WLAN packet capture in order to listen to the appropriate channel (attacked AP) and save the captured packets to the disk file. Do not specify the network BSSID number, sniffer will show you all traffic on the selected channel.

Note the name of the file in which are stored the packages: ....
!NOTE Check the files in default folder (use: *ls*). If a files with the selected name are exist in default folder, then remove the old files prior to run the sniffer.

Warning! To break the key it is necessary to capture a large number of initialization vectors IV (encrypted dada frames). This can take a lot of time, depending on the traffic in the network.

IV)

Open a another Linux console and start the program to crack WEP (use: *aircrack-ng*) indicating the name of the file with the saved packages and BSSID of the target network.

! NOTE program *airodump-ng* and *aircrack-ng* can operate in parallel in two separate consoles. In such a way that *airodump-ng* collects and stores the packets, the program *aircrack-ng* analyzes packets on-line at subsequent turns as they are being added to the file by *airodump-ng*.

V)

Wait for the moments when enough number of packages will be captured, and the password will be cracked by *aircrack-ng*.

How many packages have been use to crack the key (see: airodump-ng console)?............................
How many initialization vectors VI were collected for cracked the key? ....

VI)

Write the cracked key 64 bits ……………………………………………….

VII)

Log in to the “target-223” network with the creaked key. Check connection with ping to Internet host (eg. ping 8.8.8.8).

Remove the virtual **monitor** NIC from Linux system.

Used programs and commands:

aircrack-ng - breaking WEP security
aireplay-ng - generating additional packages, !Note aireplay-ng is not use in our scenario.
airmon-ng - settings / check card settings
airodump-ng - sniffer intercepting packets
ifconfig - configure / view the configuration of interfaces
iwconfig - configure a wireless interface
macchanger - change the MAC address

Questions:

1. How we can improve the safety of the wireless network with only WEP mode?
2. What other 802.11 network security modes you know?

References:

[1] E. Perahia, R. Stacey, “Next Generation Wireless LANs 802.11n and 802.11ac”, Cambridge University Press, 2013
[2] P. Roshan, J. Leary, “802.11 Wireless LAN Fundamentals” Cisco Press, 2004.