## Lab Report — Wireless Network Security (Assignment 7)

## Shynbolat Unaibaev

## Brief Description: This report summarizes the results of passive and targeted scanning of wireless networks, extracting RSN IEs from beacon frames, capturing EAPOL/PMKIDs, and analyzing risks. Below are detailed instructions, a network table, screenshot locations, and recommendations.

## 1. Objective

## Objective: Monitor the wireless environment, collect data on five selected networks, obtain RSN IEs and (if available) capture 4-way EAPOL handshake and/or PMKIDs, analyze the security level, and prepare recommendations for improving security.

## 2. Hardware and Software

## Adapter: USB TP-Link Archer T2U PLUS (Realtek RTL8821AU chip)

## Kali Linux (in VirtualBox, adapter drivers are working)

## airodump-ng, aircrack-ng, hcxdumptool, Wireshark, nmcli, iw, rfkill.

## 3. Brief Procedure

## 1. Check adapter visibility: lsusb (write down the line with VID:PID and name).

## 2. Install the driver if necessary (example for RTL8821AU: morrownr/8821au via DKMS).

## 3. Enable monitor mode: airmon-ng start <iface> or iw dev ... set type monitor.

## 4. Passively scan the air: airodump-ng --band abg -w capture wlan0.

## 5. Targeted capture (by BSSID and channel) to obtain EAPOL/PMKID: airodump-ng --bssid ... -c ... -w target.

## 6. Open the capture in Wireshark and take screenshots: Beacon → RSN Information; filter eapol.7. Return the system to normal mode: airmon-ng stop wlan0mon, systemctl start NetworkManager, modprobe -r <driver> (optional).

## 4. Table of selected networks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | SSID | Security Type (WPA2, WPA3, Open) | Encryption (AES, TKIP) | Notes (e.g., WPS enabled, MFP missing) |
| 1 | Jamal | WPA3 | CCMP | SAE |
| 2 | Study | WPA2 | CCMP |  |
| 3 | Office | WPA2 | CCMP |  |
| 4 | Wifi-Guest | WPA2 | CCMP |  |
| 5 | Lab342 | WPA2 | CCMP |  |

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.  
Изображение выглядит как текст, снимок экрана, Шрифт

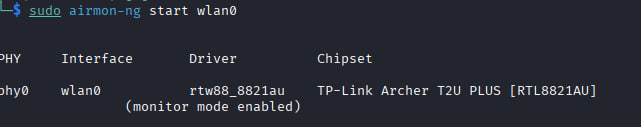
Содержимое, созданное искусственным интеллектом, может быть неверным.

Изображение выглядит как текст, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

Изображение выглядит как текст, Шрифт, снимок экрана, дизайн

Содержимое, созданное искусственным интеллектом, может быть неверным.



Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Изображение выглядит как текст, снимок экрана, Шрифт, меню

Содержимое, созданное искусственным интеллектом, может быть неверным.

**6. Vulnerability analysis (templates to fill out)**Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

We need to determine:

Pairwise Cipher Suites — (CCMP/AES or TKIP);



Изображение выглядит как текст, снимок экрана, Шрифт, информация

Содержимое, созданное искусственным интеллектом, может быть неверным.

AKM Suite — (PSK / SAE / 802.1X);

Изображение выглядит как текст, Шрифт, программное обеспечение, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

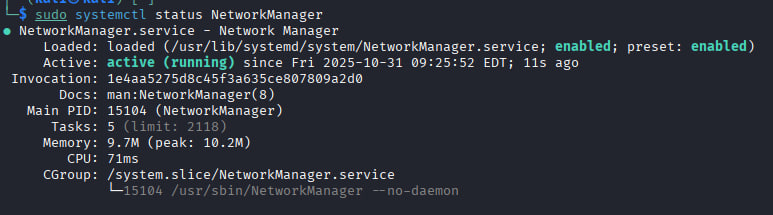
RSN Capabilities — (presence or absence of MFP);

Изображение выглядит как текст, Шрифт, программное обеспечение, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

Next, we need to apply the eapol filter to detect a four-way handshake. The screenshot shows that no four-way handshake was detected.Изображение выглядит как программное обеспечение, текст, Мультимедийное программное обеспечение, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

After completing the task, we need to reset all configurations:

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

KRACK (Key Reinstallation Attack): Description: A vulnerability in the 4-way handshake allows reinstallation of keys and decryption of traffic. Mitigations: OS/firmware updates, use TLS/VPN.

PMKID attack: Description: PMKID capture allows offline brute-force of the PSK. Mitigations: Switch to WPA3/Enterprise, use strong passwords.

Dragonblood (WPA3): Description: SAE implementation issues; Mitigations: Firmware updates, patch checks.

7. Security Recommendations

• Switch to WPA3 (where possible) or WPA2-Enterprise (802.1X) for corporate networks.

• Disable WPS on access points.

• Enable Management Frame Protection (MFP) / Protected Management Frames.

• Use long and random passphrases (PSK) of at least 20 characters for home networks.

• Periodically update AP/router firmware and client OS.