Wireless Security

Minimizing Security Risks in a Wireless LAN

Weight: 1.15% Marks:  /48

Student Name: Coleton Sanheim

Student ID: 000862545 Date: 2022-03-24

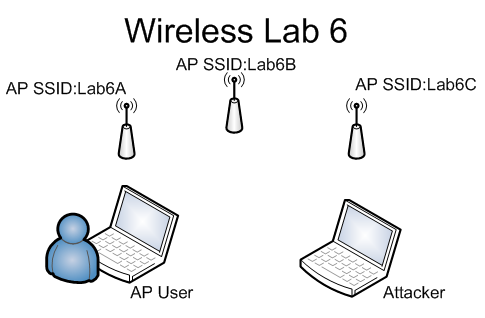
# Introduction

In this lab, you will focus on various attacks against WEP, WPA2-PSK architectures.

Lab activities in this course will be marked in class. You must bring this document to every lab in the module. Each activity must be completed and then marked by the instructor before you move on to the next. To avoid a mark of zero for an activity, contact the instructor immediately if you cannot complete the activity for any reason, or if the activity was left unmarked by the instructor.

# Equipment

* TP-Link AP
* Wireshark with WINpcap
* Kali Linux
* Laptop with 802.11 and Bluetooth wireless
* Topology



© 2017, Southern Alberta Institute of Technology

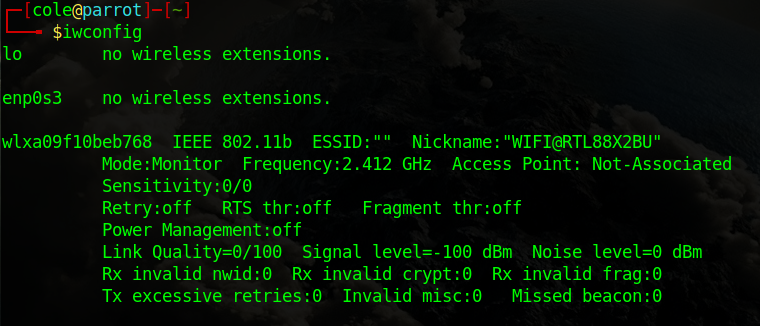
# Lab Setup

Before you begin the lab activities, set up a Windows workstation with the following parameters:

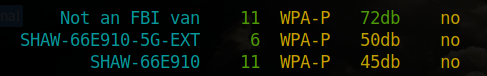
* Wireless network adapter
* WiFi Inspector
* Latest version of Wireshark with Winpcap

# Activity 6.1: Verifying Wireless Network Functionality

1. Verify that the wireless network is functioning by accessing the wireless AP interface.   
   (2 points)



**The adapter is recognised and in monitor mode**

****

**The two AP’s I am targeting is Not an FBI van (my mobile hotspot) and SHAW-66E910 (my home network)**

**Instructor sign-off:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (5 points)

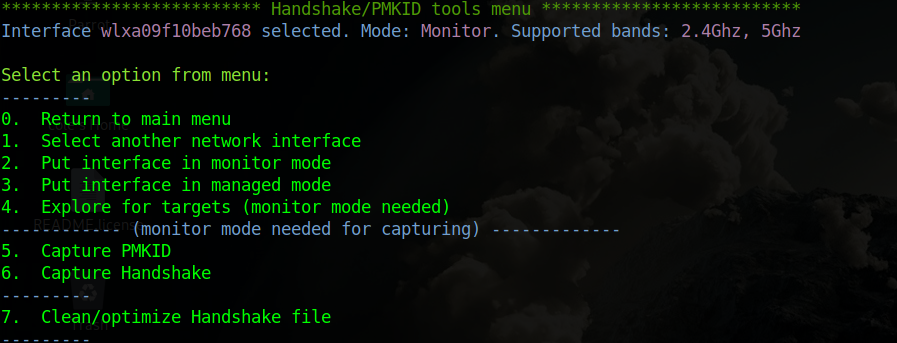
# Activity 6.2: Testing from Kali to Recover Keys

1. What channel was used for each AP? (6 points)

* AP SSID:Lab6A: **11**
* AP SSID:Lab6B: **11**

1. Describe the tool and commands used for each detection. (6 points)

* AP SSID:Lab6A: **airgeddon, using option 5 handshake detection.**
* AP SSID:Lab6B: **airgeddon, using option 5 handshake detection.**

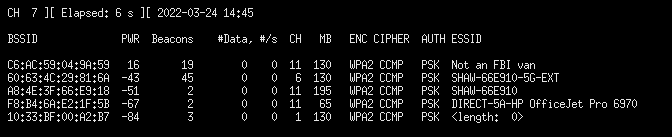


1. What type of encryption protocol was used for each AP? (6 points)

* AP SSID:Lab6A: **WPA2**
* AP SSID:Lab6B: **WPA2**

1. Describe the tool and commands used for each detection. (6 points)

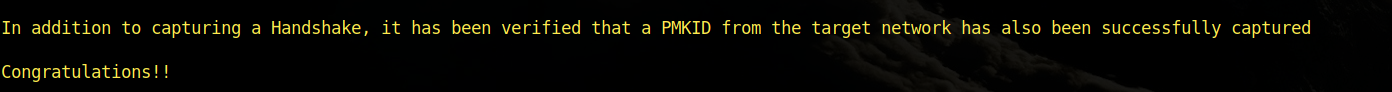
* AP SSID:Lab6A: **First I captured the handshake, then I used the captured handshake file to crack the key. All from the airgeddon command.**
* AP SSID:Lab6B: **First I captured the handshake, then I used the captured handshake file to crack the key. All from the airgeddon command.**



**Detection running on possible networks**

1. What keys were recovered from each AP? (6 points)

* AP SSID:Lab6A: **No key was found, I even tried the capture multiple times and included the password directly in the dictionary file but no key could be found.**
* AP SSID:Lab6B: **The correct password key was found**







1. Describe the tools and commands used for each detection. (6 points)

* AP SSID:Lab6A: **Again, I just used the airgeddon tool to crack the handshakes, using the WPA handshake cracker included in the command.**
* AP SSID:Lab6B: **Again, I just used the airgeddon tool to crack the handshakes, using the WPA handshake cracker included in the command.**

**Instructor sign-off:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (5 points)