Wireless Security

Insecurities and Threats in WLAN

Weight: /1.15% Marks: /18

Student Name: Coleton Sanheim

Student ID: 000862545 Date: 2022-02-18

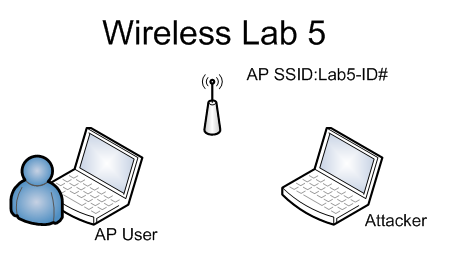
# Introduction

In this lab, we focus on implementing TKIP with WEP and collecting and reviewing wireless traffic.

Lab activities in this course will be marked in class. You must bring this document to every lab in the module. All activities 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 for any reason you cannot complete the activity or if the activity was left unmarked by the instructor.

# Equipment

* TP-Link AP
* Wireshark with npcap
* Kali Linux with various tools
* Laptop with 802.11 & Bluetooth Wireless
* Topology



© 2017, Southern Alberta Institute of Technology

# Lab Set Up

Before you begin the lab activities, perform the steps below to set up your computer.

1. Set up a user workstation the following parameters:

* Wireless Network Adapter using WEP TKIP
* Latest version of Wireshark with Npcap
* Ensure AirSnort, WEPCrack, and dweputils are installed on Kali

1. Set up wireless AP with the following parameters:

* Implement TKIP over WEP (WPA/802.11i) networks including keying, message integrity checks (MIC), IV sequencing
* SSID:Lab5-(StudentID#)
* Passphrase: ISSStudent2019

## Instructor Demo

## 802.11z "Direct Link Setup"

Instructor will perform an on screen demo of an 802.11z direct link connection from one computer/device to another

**See screenshots below**

## 802.11ac "Gigabit over WiFi",

Instructor will perform an on screen demo of an 802.11ac Gigabit over WiFi connection from a computer/device to access point

**See screenshots below**

## 802.11af "WiFi in TV White Space"

Instructor will perform an on screen demo of an 802.11af Wifi connection in TV White Space

## Bluetooth

## Instructor will perform an in class demo of an Bluetooth piconet

**See screenshots below**

## Lab Activity 5.1: Verify that the wireless network is working

Perform this test by accessing the wireless AP interface wireless. (2 points)

Applying TKIP failures to modern cryptographic systems. (2 points)

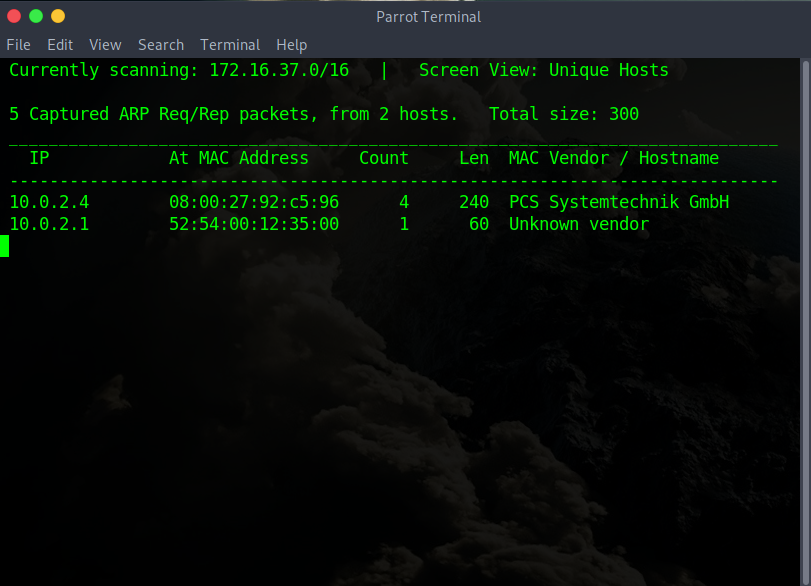
**Instructor sign-off:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (5 points)

## Lab Activity 5.2: Perform testing from Kali to recover the key used

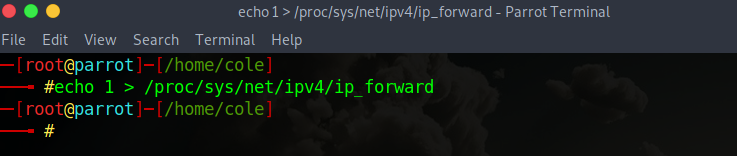
1. What the keys recovered: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (2 points)
2. Describe the tool and commands used: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (2 points)

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

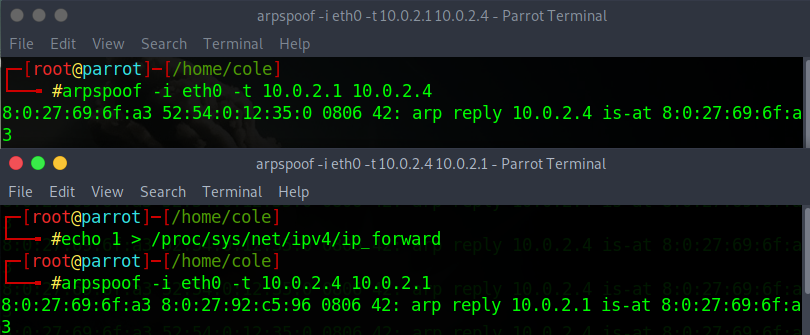
**Part 1:**

****

Using netdiscover to discover potential targets

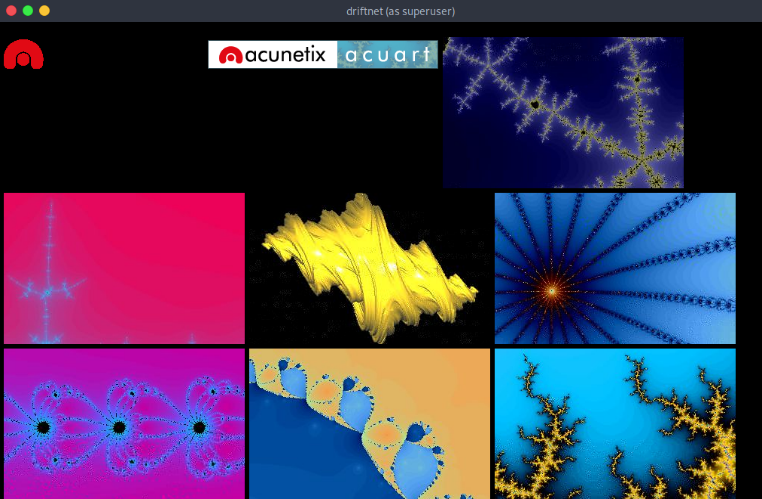


Changing the ip\_forward settings

running the arpspoof command on two different terminals

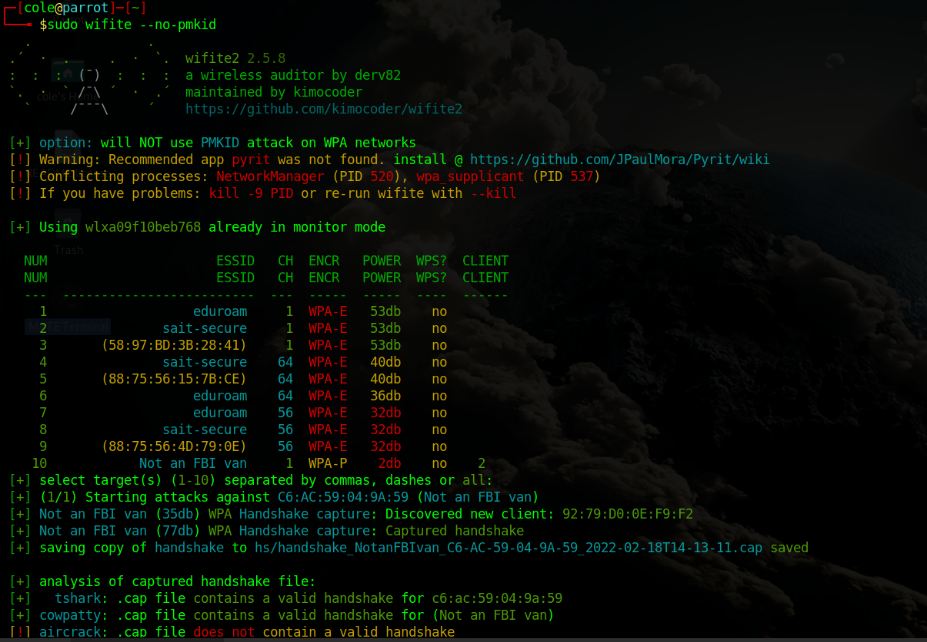


Running driftnet to capture images

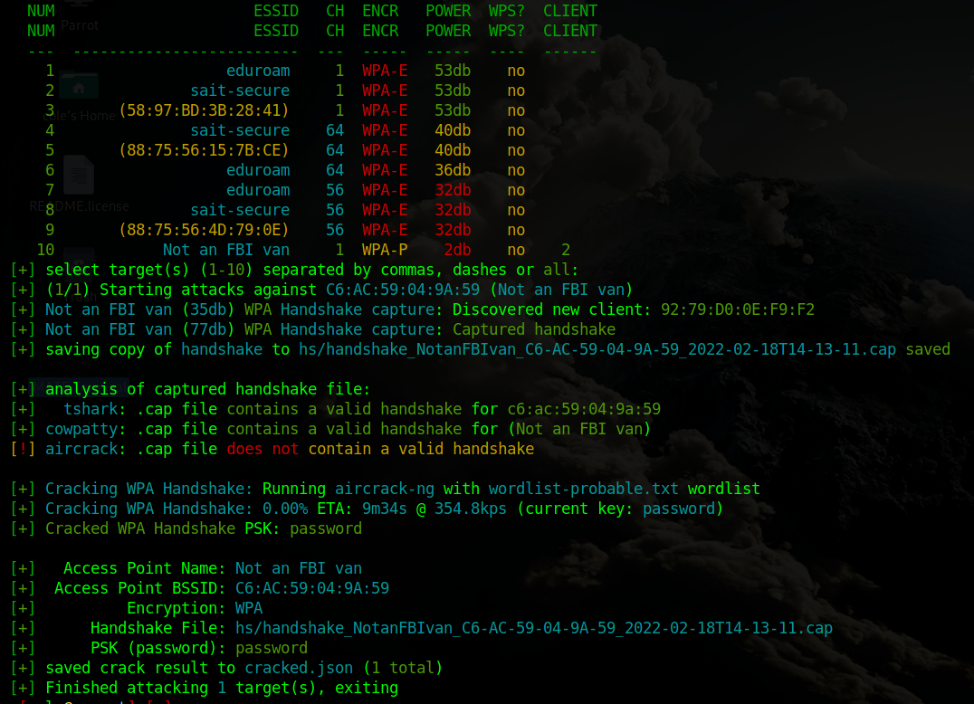


Captured images

Part 2:

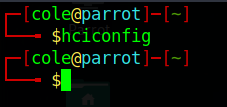


Running wifite and discovering a network (not an fbi van, which is my mobile hotspot)



The successful crack of my password (which I set to be password so its easy)

Part4:



The command hciconfig to display Bluetooth devices does not display any devices, as such my machine is not Bluetooth capable, so I am unable to complete this part of the lab.