WiFi Hacking Project

Team of 2 (max)
(76 points)

0. Learning Objectives

- Practice WiFi scanning and reconnaissance
- Exploit WEP access points with connected clients
- Exploit WEP access points with different key sizes
- Exploit WPA2 access points
- Optional: Teamwork!

1. Project Introduction

The focus of this project is WiFi hacking. You will exploit wireless access points with different settings. This project will require research before performing the exploitation. The success of your technique highly depends on being physically close enough to send and receive access point packets.

You must use the Kali machine assigned to you in the Pitt Cyber Range. You will find a "`Ralink Technology, Corp. RT5572`" adapter attached to your assigned machine. Use that machine to work on this project.

Note: You can work on this project alone or with (ONLY) one other student in the same course.

2. Problem Statement

Find the essid, channel, manufacturer, and key (a.k.a. password) for the following WiFi access points:

- ORLANDO
- BERLIN
- Vancouver (the 'names.txt' wordlist)

Good luck!

*** Section 3 below has useful hints and references. Search engines are useful too!*

3. Hints and References

- You are highly encouraged to work with another student on this project. You can have one of your machines listening to the wireless communication and the other machine performing the exploitation.
- If you can't find ORLANDO or BERLIN, check this.
- Never use `aireplay-ng` in this part of the project.
- Don't `DEAUTH` any clients in this project. Otherwise, you are preventing everyone from completing this project.
- Exploiting the above-mentioned APs has been tested and verified using this Kali VM and the Panda PAU07 "`Ralink Technology, Corp. RT5572`" wireless card.
- If you use a different wireless card or OS for the exploitation, we can't guarantee the success of your exploitation.
- Crack one access point at a time — your adapter can't handle listening on multiple channels
- Tutorial: WEP Cracking
- Tutorial: Simple WEP Crack
- Interesting news article: Israeli Researcher Cracked Over 3,500 Wi-Fi Networks in Tel Aviv City