Lab04- 802.11 Parsing

Leveraging currently available tools in a security aspect makes our lives as security researchers much easier. However, the situation may present itself that results in current tools being unable or inefficient for the task that is at hand. In this lab, we will explore the creation of our own 802.11 frame parser that will be used to collect data for analysis.

Overall Goals

We will create a tool that will attach to a WLAN adapter that is in monitor mode (feel free to include logic to handle monitor mode, if you wish) and capture 802.11 frames so that we can programmically parse the data. Once we have the data, we will have flexible options for what to do with it, perhaps we just need to filter or display it to the screen, the potential exists where we may just need to quickly count how many frames of a certain criteria exist, or perhaps we will format the data in a JSON format to be shipped to an external tool. Regardless of the intended output, having our own tool will allow us the flexibility to meet future needs.

Basic Requirements

Using Python and Scapy (or a language/framework of your choosing), create a tool that captures 802.11 frames.

Within the tool, filter the frames so we're only working with 802.11 Beacon frames

Once you've filtered captured data down to just Beacons, parse the beacon for the following information & display it to the screen:

- ESSID
- BSSID
- Timestamp
- Beacon Interval
- Other fields of your choosing

What to Submit

- Submit a screenshot of your tool running and happily capturing frames as well as the code for your tool. If you're one of those crazy kids that used something aside form Python—that's cool. Tell me a little about your tool then, how it works, etc!