Wardriving

- Due Jan 23 by 11:59pm
- Points 100
- Submitting a text entry box
- Available Jan 7 at 12am - Apr 30 at 11:59pm 4 months

Note: This lab should be conducted on a machine with a working wireless network card.

Also note: I have used some of these applications for years and have never had a problem (virus, spyware, etc.) with them. Still, assessing them with an anti-malware scan is always the safest idea. Beware any homebrew applications that are available online.

Final Note: Avoid using Kismet or any similar packet capturing software. We want to detect, not collect.

One of the most popular free applications that can be used with wireless networks is network locating software. To complete this assignment, you will need to use software of this nature. Using the software will give you information about the networks around you, including whether or not certain networks are utilizing security features. If you do utilize this software, **do not try accessing any of the open networks** you will likely find. That could well be illegal in your area.

- If you use Windows XP, you can download and install the “NetStumbler 0.4.0” software at netstumbler.com (Links to an external site.)Links to an external site.. It is located under the Downloads link at the top of the page.
- If you use Windows 10 (and 7, 8, and Vista), try “Vistumbler v10.6.4” at vistumbler.net (Links to an external site.)Links to an external site. . The download link is at the very top of page. I have been unable to test this with Windows 8.
- For Mac users, Apple offers AirRadar 3.1.9 at https://itunes.apple.com/us/app/airradar/id414758651?mt=12 (Links to an external site.)Links to an external site.. This used to be free, but now Apple appears to be charging $9.99 for it. Try to avoid doing this if you can (unless you think it would be fun to own).

There may be free options available for your mobile devices. Consult iTunes, Google Play, or whatever app market may apply. I cannot personally vouch for anything other than the three above though.

Windows XP: NetStumbler The screencap shows the blank slate that you begin with. Once your wireless NIC has been detected, NetStumbler should automatically begin locating wireless APs within range. If it doesn't start automatically, click the green "Play" button.	NetStumbler Image not found or type unknown
Vistumbler The Scan APs button in the top left corner will begin the search for wireless networks.	Vistumbler Image not found or type unknown
AirRadar (for Mac) The Start Scan/Stop Scan button is in the upper right corner. Pretty straight forward.	AirRadar Image not found or type unknown

As you'll see, there will be a number of rows and columns that will soon populate. Some of the columns include:

MAC Address: The unique identifier for the AP network interface card.

SSID: Service Set Identifier, also known as the "network name."

Encryption: The type of security implemented on this particular wireless network. This may include WEP, WPA, EAP, or something similar.

To submit the assignment, please report the following information below:

- Date of the wardrive
- Location of the wardrive
- Software and device used
- In percentages:
  - How many of the detected networks have the default SSID (i.e. it has not been changed by the owner)?
  - How many of the detected networks had some type of encryption enabled?
- What different channels are the detected networks broadcasting on?
- Judging from info you gathered, how many 802.11 a, b, g, n, and ac networks did you detect?
- Any other observations or strange occurrences to report?

Revision #1
Created 9 January 2019 20:16:48 by Aaron Kimbrell
Updated 9 January 2019 20:17:52 by Aaron Kimbrell