Assignments

- Wardriving
- Network Address Translation
- Shodan

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 not found or type unknown
Vistumbler The Scan APs button in the top left corner will begin the search for wireless networks.	Vistumbler not found or type unknown
AirRadar (for Mac) The Start Scan/Stop Scan button is in the upper right corner. Pretty straight forward.	AirRadar 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?

Network Address Translation

Instructions: Run a test of your network address translation using the instructions on page 549 of our textbook. You will need to be connected to a network.

Please report your results for the assignment. There are no right or wrong answers, so report your results faithfully, whatever they may be.

1. Define Network Address Translation.
2. What is the IP address of the computer you are currently working on?

   - Use the cmd program, *ipconfig* on Windows computers.
   - Use the Terminal program, *ifconfig* on Mac OS

3. Is this IP address within the range of private addresses on page 550?
4. Go to IPChicken.com (Links to an external site.)Links to an external site.. What IP address do they report for your computer?
5. Do the two IP addresses match?
6. So, are you running under NAT on your current computer?
7. Any interesting/surprising observations?

More info for Mac iOS users (thanks to Mia Woods and Brooke McKee for bringing this up)

Depending on the age of your Mac, your IP address info may be displayed in different places (see image below). I have an elderly (> 8 years old) MacBook at home that displays info in the opposite location in ifconfig than where your newer Mac (< 5 years old) does. I both enabled WiFi and plugged it directly into my router with a patch cable so you can see the multiple entries below.

NAT_iOS_ports.png
Image not found or type unknown

For newer Macs, your WiFi information should be listed under the en0 entry. The IPv4 address is listed next to "inet". The entries are flipflopped on my dinosaur MacBook, but since both entries display internal IP addresses, it doesn't really matter... NAT is enabled either way. You will likely see two internal IP addresses or two "real" IP addresses if you have two connection entries, so use either one for your homework. (If you only have one connection entry, that probably means that only your wireless card is currently being used.)

Shodan

Shodan Vulnerability Assessment & IoT

The Shodan website is a "search engine for Internet-connected devices." There are a ton of connected devices out there that are constantly broadcasting data, video, audio, etc. This probably does not come as a huge surprise in general, but maybe it hits a little harder when the devices are close to home. This assignment will attempt to look at some IoT devices that you are personally aware of.

Instructions

1) Go to the search engine at [shodan.io (Links to an external site.)Links to an external site.](https://shodan.io)

2) You don't have to log in to run an assessment, but it helps provide more comprehensive search returns, like the maps. I logged in with my Google account, but Facebook, Twitter, etc. logins are also available. The Login button is at the top right.

Device are located and identified by the content of its "banner" object. This is metadata that is publicly transmitted and includes things like SSIDs, IP addresses, etc. You should use filters when you perform a search, otherwise your search returns will be limited by the contents of a device's banner. Filters include "country:", "org:", "city:"

3) **Freestyle Search:** Search your hometown or something "close to home." Example: city:Starkville

4) Report what you find. Can you identify any businesses, individuals, etc? What type of data seems to be broadcasting?

5) **Third Floor Search:** Run a second search, this time the IP address 130.18.86.48. What device is this? Can you tell when the SSL certificate expires on this device?

6) Now search 130.18.86.47. What about its SSL certificate?

Like most search engines, you sometimes find results that are relevant to what you are attempting to find and sometimes you don't, but that is the spice of life, isn't it?