Cyber Visualization (CyVis)

Daniel Baldwin, John Cotham, Joseph Raetano, George Rhinehart

[Overview](#h.f4gic0berjtw)

[1. What is the problem being addressed?](#h.1quhzbli7ua)

[2. Who would be the interested parties that would want to understand the data better?](#h.rzpqq9d2mtxn)

[3. Where is the data coming from and what are its characteristics?](#h.s6tt4r5avts5)

[4. Make sure the data and its attributes are described in detail.](#h.sucbzod491pe)

[Tutorial](#h.jtbdmg6btpez)

[Installation](#h.ulppegbf7zw7)

[Running the application](#h.qtzoo0x66ymf)

[Description of Visualization](#h.t6r8addsl5zp)

[Ultimate Goal](#h.kvgvw3cxsgax)

# Overview

## 1. What is the problem being addressed?

Computer and Computer Network data is often hard to visualize since there is a limited amount of information available in any given application or screen. Making the data available in a common, easily understood and universally accepted format can make the data easier to visualize and correlate. In our project, we will attempt in a pedagogic manner to showcase various computer and network information in a new and enlightening way to improve the cognitive ability of the interested parties.

**1) network maps (network flows, network devices, network users),**

**2) Quality of Service (QoS),**

**3) assist in planning network setup, upgrade and maintenance**

**4) routes to servers and services on Intra-Internet.**

## 2. Who would be the interested parties that would want to understand the data better?

Users, System administrators, Network Engineers, Network Planners, Cyber Security Teams, Students, Educators

## 3. Where is the data coming from and what are its characteristics?

Most of the data will be parsed from tools already on most operating systems. We are planning on the initial prototype being a Linux based distro. Some of the initial applications that we will capture data from will be: **ifconfig, netstat, whois, ping, and traceroute.** We’re looking at other computer and network related data from applications such as **Nessus, Nmap,** and **snort** as well.

## 4. Make sure the data and its attributes are described in detail.

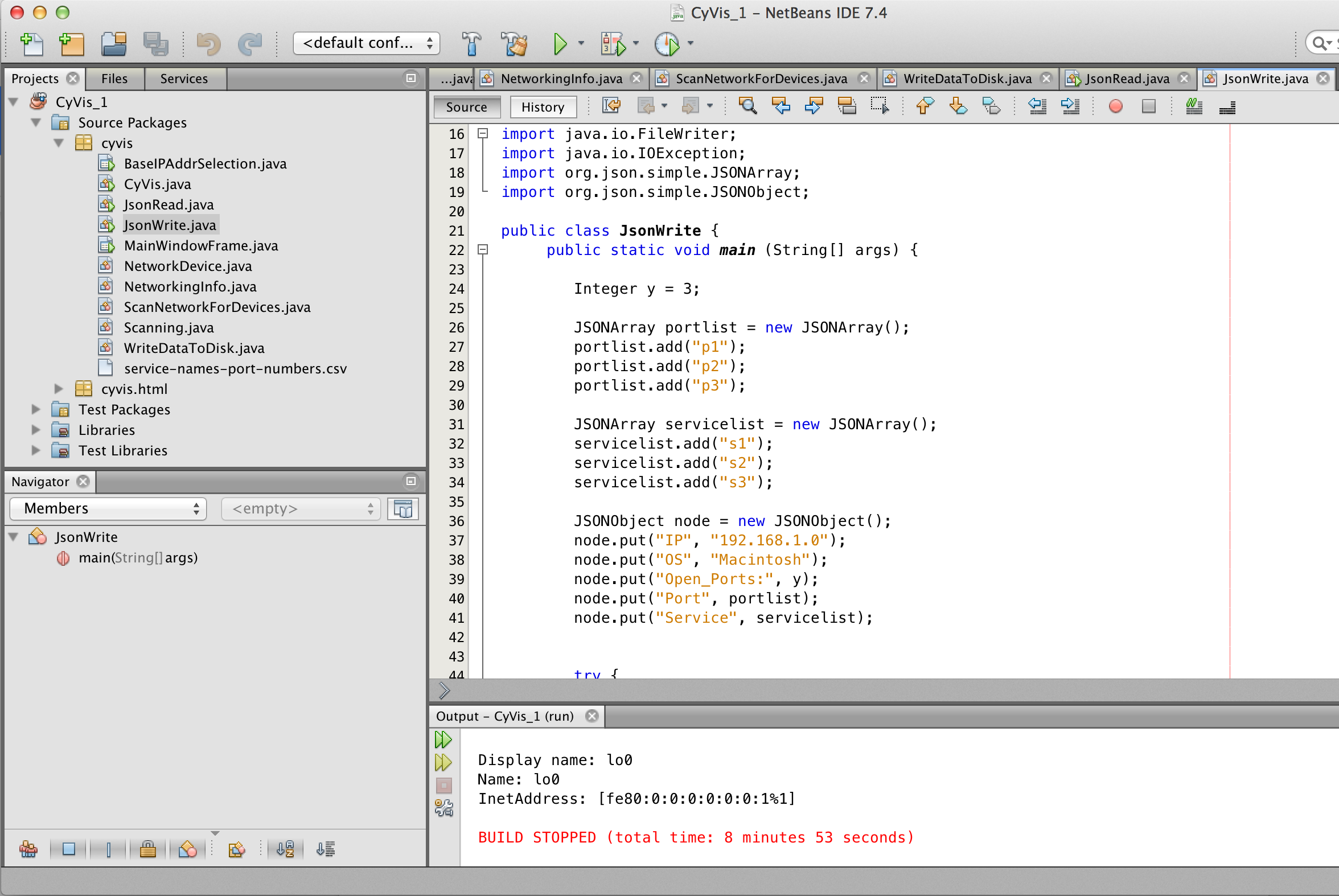
We plan on parsing the data into a text file, tab/comma/space delimited. There is a wide range of network data available, such as:

* Network Addresses
* Inbound and outbound connections (as well as number of connections per IP)
* Routes (obtained from traceroute - What path does the network traffic follow)
* Total packet times
* Total data sent and received
* Geolocation data (from whois)
* Open ports and services (UDP, TCP, obtained from nmap)

# Tutorial

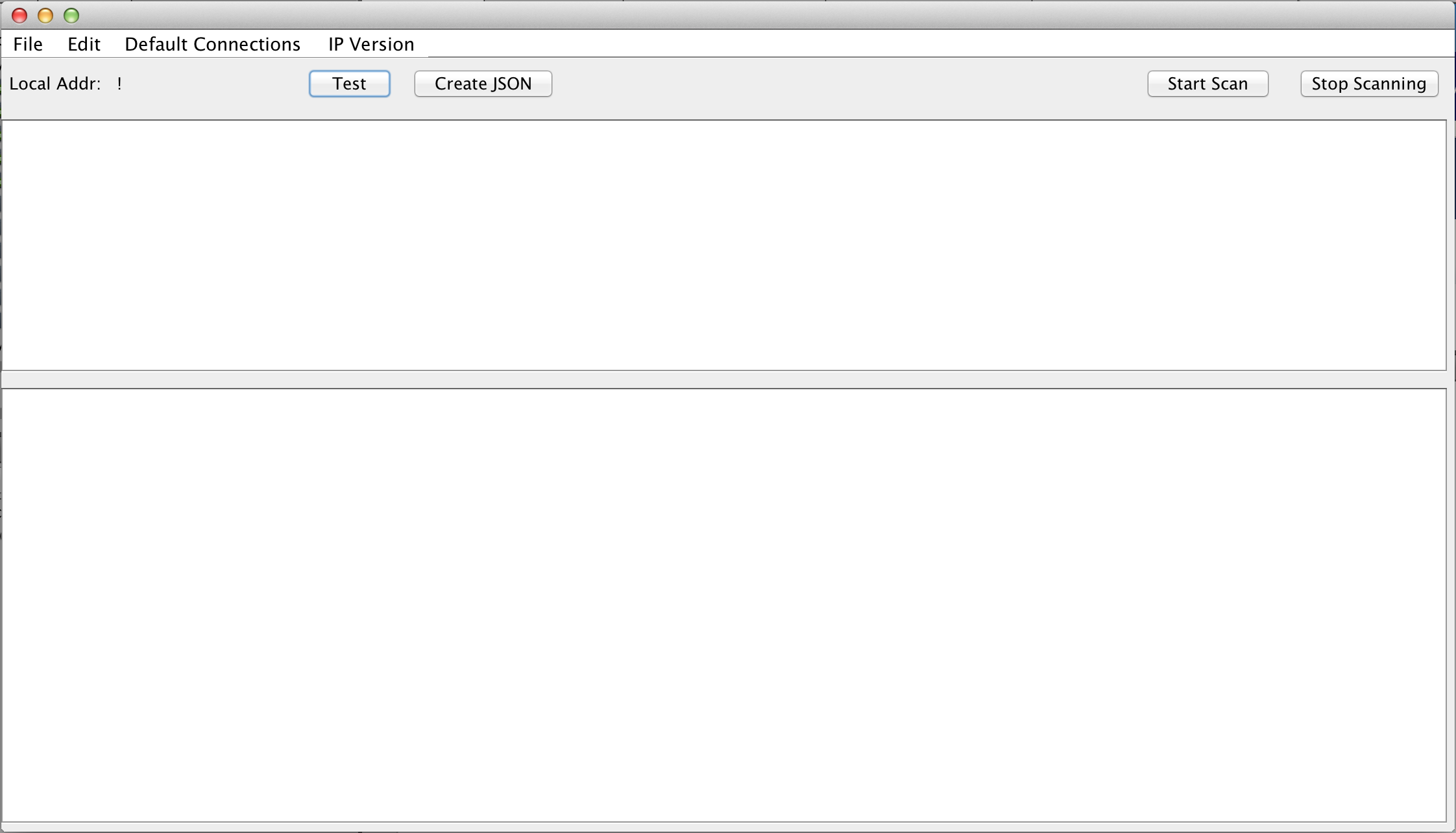
## Installation

1. Log into github and pull down the CyVis\_1 NetBeans project in a local folder: <https://github.com/CyVis/drunken-ninja/tree/master/CyVis_1>
2. download and install Netbeans from <https://netbeans.org/downloads/>
3. download and install nmap from <http://nmap.org/download.html> ensure you are able to have root or admin priviledges.
4. If you’re on a Mac run Start Netbeans like this “sudo open /Applications/NetBeans/NetBeans\ 7.4.app/” and open the NetBeans project you just downloaded.

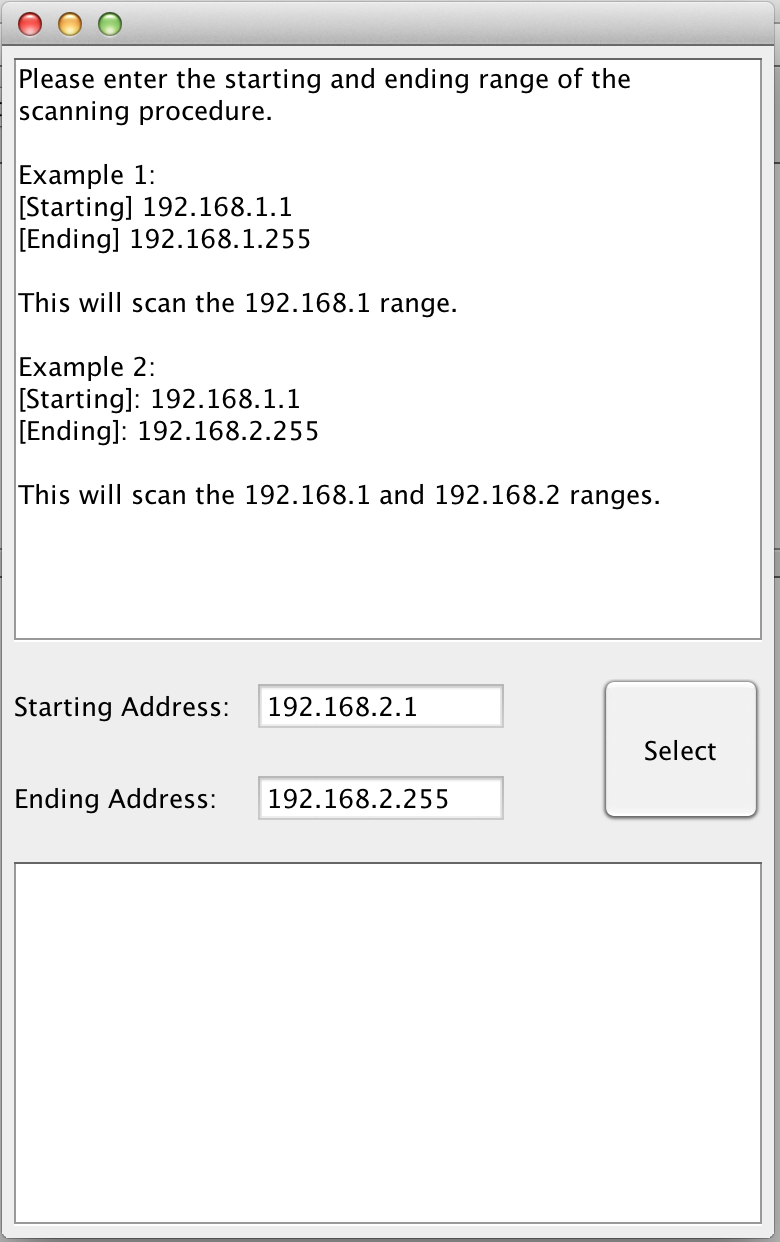


1. Next run the project, the application should start

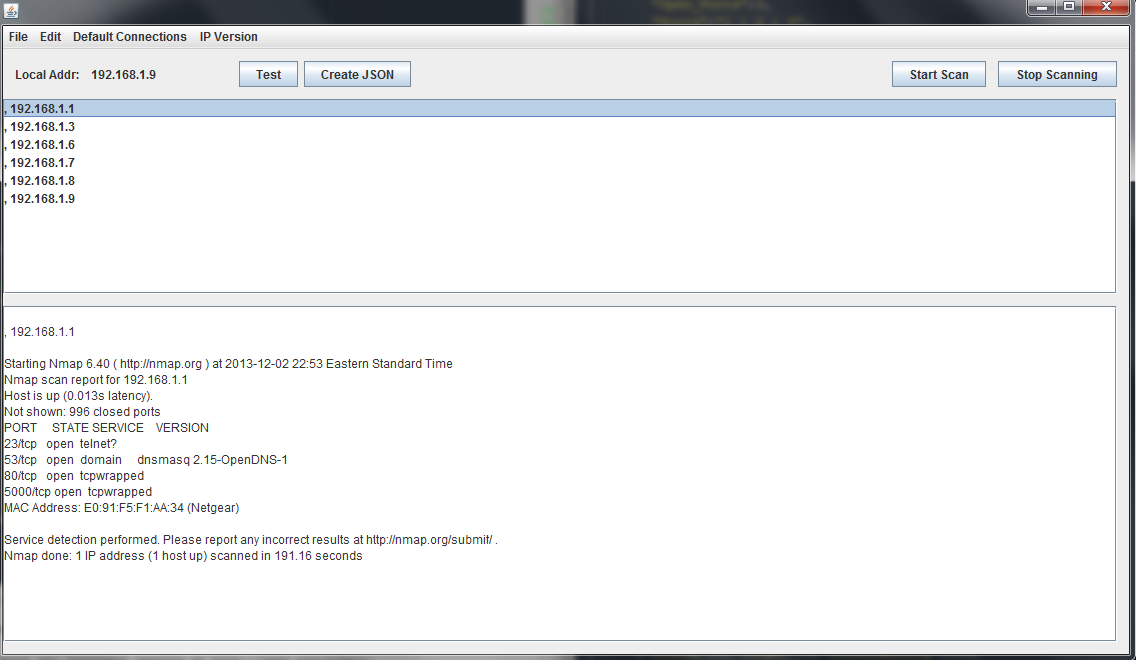
## Running the application



1. Click edit and set the scan range of your network



1. Next, click “Start Scan”

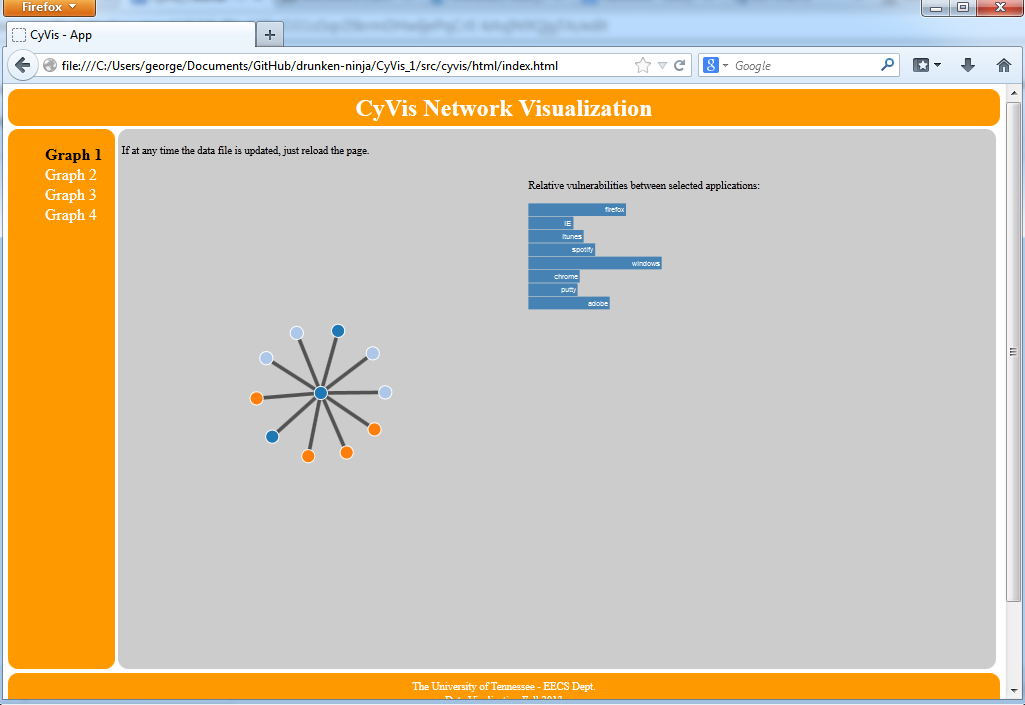


1. Now, to view the network data you must direct your browser to the directory containing the index.html file. For example: file:///C:/Users/george/Documents/GitHub/drunken-ninja/CyVis\_1/src/cyvis/html/index.html

## Description of Visualization

The visualization in the web page is interactive, as it allows for mouseover, clicking, and dragging events. Also, the webpage has only been successfully tested using the Firefox browser. (To download the Firefox browser, go to [http://www.mozilla.org](http://www.mozilla.org/en-US/firefox/new/?utm_expid=71153379-28.ZuzIY8GHTdmX0QtrDFcQLQ.0&utm_referrer=https%3A%2F%2Fwww.google.com%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3D%26esrc%3Ds%26source%3Dweb%26cd%3D1%26ved%3D0CC8QFjAA%26url%3Dhttp%253A%252F%252Fwww.mozilla.org%252Fen-US%252Ffirefox%252Fnew%252F%26ei%3DvGCdUrbuC4i6kQfI1YCwDg%26usg%3DAFQjCNHXR7GrDNHIc3plcSvQSx_ByCacYQ%26sig2%3DIIhPaOaFjF6VTPGP94XYXg%26bvm%3Dbv.57155469%2Cd.eW0))

The visualization shows nodes in a network, color coded by whether they have suspect ports open. Nodes with suspect ports are flagged red. The bar graph on the right shows additional information pulled from Mitre’s Common Vulnerabilities and Exposures database that highlights vulnerable applications that may be running.



# Ultimate Goal

Our ultimate goal was to have the ability to visualize vulnerability data and correlate it with local scan data. This goal is a work in progress. We had two aspects to this project: 1) collect data using our own java application, and 2) visualize the data using d3 in a browser. We cannot call this a finished project, but merely the prototype of “what-could-be”. There was just not enough time to do all the things we wanted to do, like showing network traffic and packet analysis, and using geolocation data from the “whois” command.

Future versions of the software would implement dynamic checking against publically available vulnerability databases. Since our application currently pulls network services and OS (when applicable) having this dynamic checking in place would be a powerful tool for near real-time vulnerability analysis.