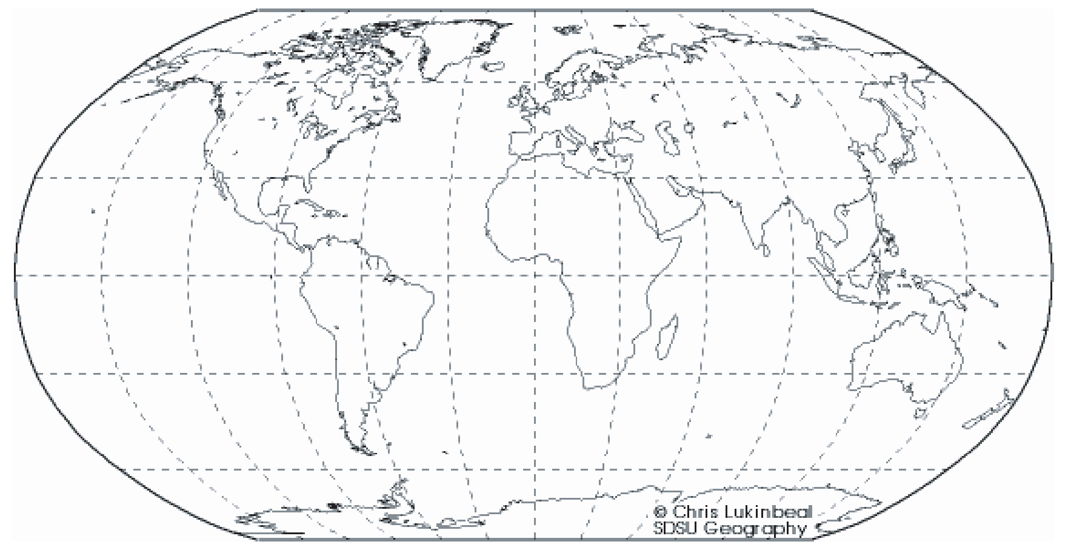
Detection of Port Scanning

S. Mazul, R. Simpson

gtg820q@mail.gatech.edu, rsimpson@ece.gatech.edu

Introduction

For the 2004-2005 school year, my mentor, Robby Simpson, and I have been looking at network port scanning. The main reasons port scans occur are either for hacking or virus invasion. We decided to check over the Neti@home user information and by changing either time span or number of ports in the code obtained various results to analyze.



Background

Neti@home is an open source software package that collects network performance statistics from the system. The information is sent to the MANIACS lab at Georgia Tech, after permission is granted by the user, where it is then analyzed and improvements are then made to Neti@home that would better help the user and the results are published.

www.neti.gatech.edu

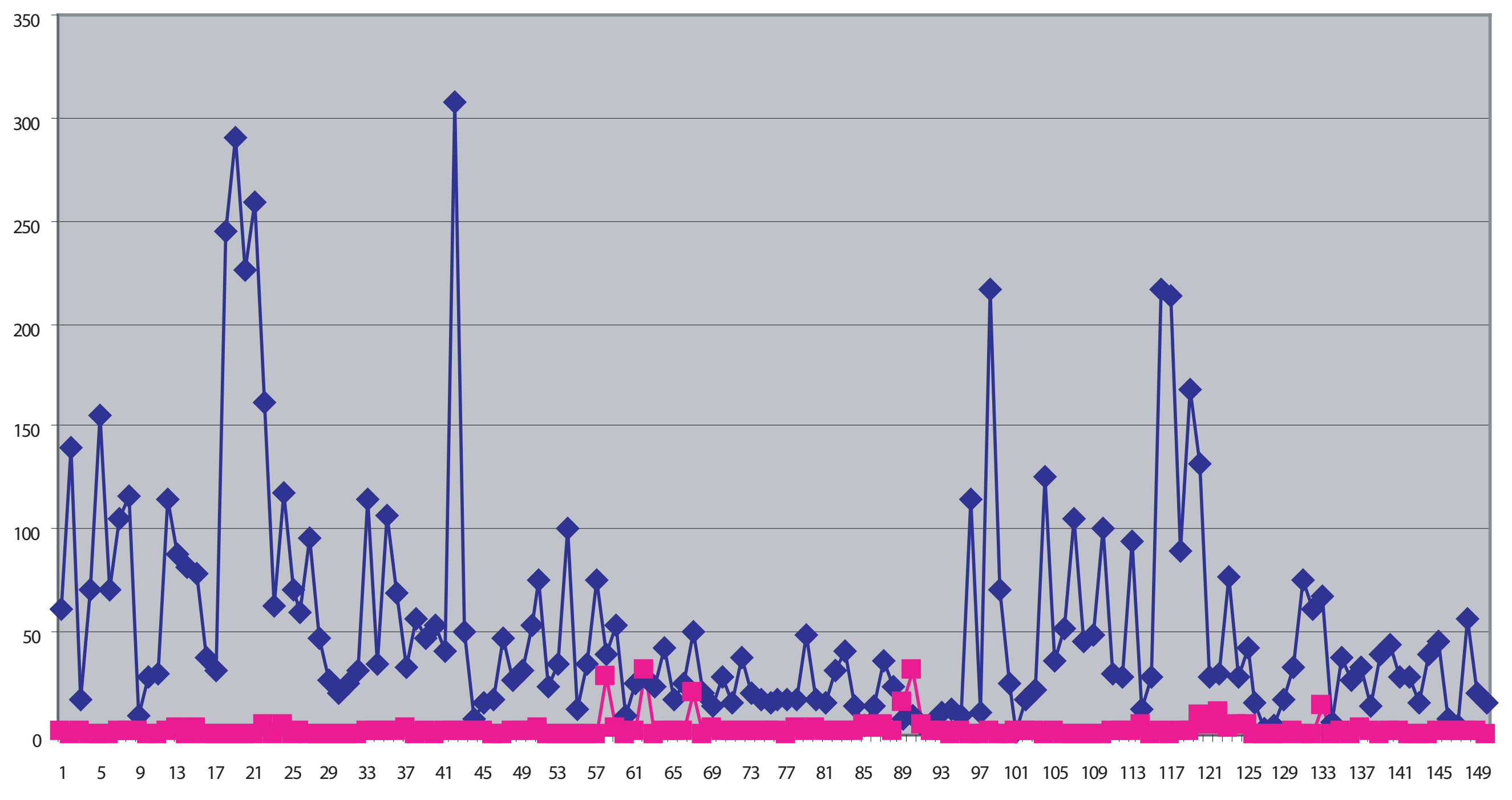
Methods

The following is the brief step by step process that was used in this project:

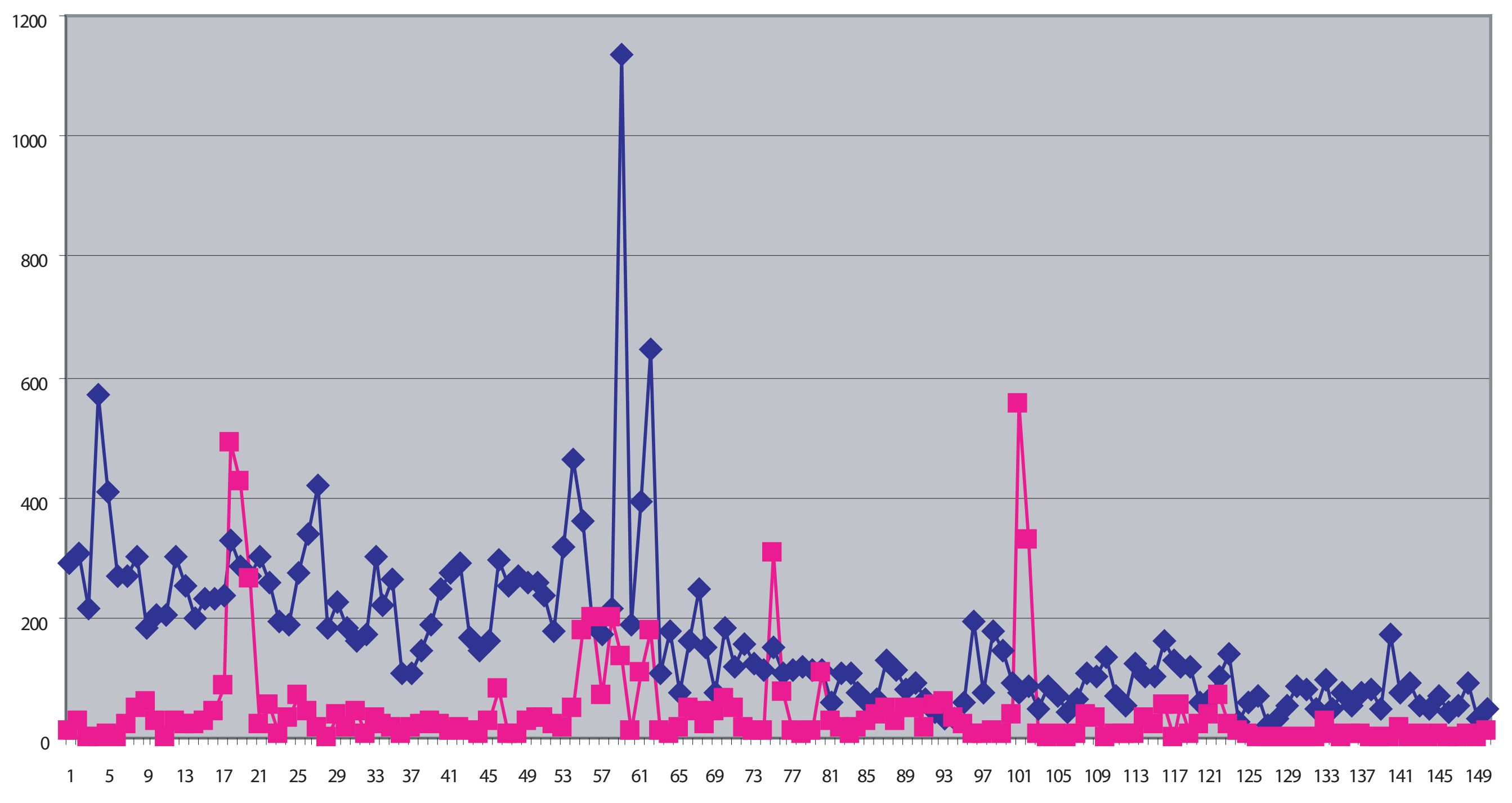
- develop code to check for scans
- run 4 months worth of data through
  - data gathered from Neti@home users
- analyze the data

Results

- Average Users A Day = 18
- Average TCP scans:
  - 1 second = 55
  - 60 seconds = 167
- Average UDP scans:
  - 1 second = 2
  - 60 seconds = 42



# ports = 25
time span = 1 second



TCP – dark blue
UDP - pink

# ports = 25
time span = 60 seconds

Conclusions

By using the same remote IP's and examining x ports within a y time span we were able to reach the following conclusions:

- port scanning happens a lot regardless of the port/time combo
- TCP scans are more frequent than the UDP
- varying the port and time variables makes a difference in the outcome
- since the average per day is greater than 1, odds are that everyone is scanned everyday

Future Work

In the future my mentor and I have discussed investigating the anomalies that occurred on some days where the actual result did not match with the theory. Also, we would like to look at finding an optimal port/time combination.