

HOMEWORK #1

1. Go to www.sans.org and print out the first 10 (only the first 10!) of the SANS top 20 list.
2. List the full path to the log file on your computer in which failed logins are recorded. Be sure and tell me what OS you are running.
3. List the programming language(s) you are comfortable programming in.
4. List the mathematical packages (MATLAB, R, Mathematica, etc) you are comfortable with.
5. Write a program that takes the following data and plots a scatter plot of time against SIP. You will need to convert the SIP to a 32 bit number prior to plotting.

TIME	SIP	DIP
986314699.201556	211.108.223.149	139.114.21.167
986314701.751571	211.108.223.149	139.114.21.167
986314709.340838	211.108.223.149	139.114.21.167
986314721.770638	211.108.223.149	139.114.21.167
986314909.102442	227.110.68.58	139.114.28.230
986314912.049329	227.110.68.58	139.114.28.230
986314918.082574	227.110.68.58	139.114.28.230
986315253.171677	223.194.237.225	139.114.195.3
986315256.142975	223.194.237.225	139.114.195.3
986315262.142141	223.194.237.225	139.114.195.3
986316197.990830	227.110.68.58	139.114.212.62
986316200.961802	227.110.68.58	139.114.212.62
986316207.001352	227.110.68.58	139.114.212.62
986316259.259656	211.111.222.84	139.114.196.234
986316264.878304	211.111.222.84	139.114.196.234
986356901.550050	219.245.207.82	139.114.49.210
986356904.568248	219.245.207.82	139.114.49.210
986356910.573393	219.245.207.82	139.114.49.210
986356922.650432	219.245.207.82	139.114.49.210
986359449.124640	158.18.178.242	139.114.157.216
986359458.009165	158.18.178.242	139.114.157.216
986359470.016254	158.18.178.242	139.114.157.216
986360268.610528	215.40.31.196	139.114.1.139
986360271.584244	215.40.31.196	139.114.1.139
986360277.585987	215.40.31.196	139.114.1.139
986360289.629326	215.40.31.196	139.114.1.139
986360333.903879	214.205.164.183	139.114.18.4
986367296.511647	222.145.198.172	139.114.156.58
986367306.171846	222.145.198.172	139.114.156.58
986367954.977979	222.145.198.172	139.114.103.188
986367957.988276	222.145.198.172	139.114.103.188
986367964.248932	222.145.198.172	139.114.103.188
986368909.009232	222.145.198.172	139.114.231.86
986368912.038040	222.145.198.172	139.114.231.86
986369118.044251	222.145.198.172	139.114.190.29
986369121.071581	222.145.198.172	139.114.190.29
986369127.231922	222.145.198.172	139.114.190.29
986369183.475591	222.145.198.172	139.114.152.153

```
986369186.515377 222.145.198.172 139.114.152.153
986369192.796103 222.145.198.172 139.114.152.153
986369407.098884 222.145.198.172 139.114.220.233
986369412.296937 222.145.198.172 139.114.220.233
986369418.473828 222.145.198.172 139.114.220.233
986369854.020201 222.145.198.172 139.114.35.119
986369857.576583 222.145.198.172 139.114.35.119
986369863.961556 222.145.198.172 139.114.35.119
986370304.747308 222.145.198.172 139.114.135.101
986370310.973845 222.145.198.172 139.114.135.101
986370977.409675 222.145.198.172 139.114.206.162
986370986.527387 222.145.198.172 139.114.206.162
```

Provide a listing of the code that produced the plot, including the routine(s) you used to read the data. Tell me what package/language you used.

6. Do a web search for the most current worm or virus. Report the name of the worm/virus and give a sentence or two describing it. Provide the date of the newest attack, the first sighting of the virus/worm, or any other information showing how current your information is. Provide the link to the single most informative page you have found (provide only ONE link!).

7. Computer A (IP=10.10.23.5) connects to computer B (IP=10.10.34.17) for a web session (port 80), using source port 1724. Write a tcpdump filter which will capture all the packets in this session.

8. What do the following tcpdump filters do?

- a) tcp and net 10.10. and not (dst port 80 or src port 80)
- b) ip and ip[4:4]>10000
- c) tcp[4:4] = tcp[8:4]
- d) tcp[4:2] = tcp[8:2]
- e) udp[2:1] < 255