Pdf document of documentation of previous research paper on graph representation of anomalies

<http://users.csc.tntech.edu/~weberle/EberleIDA07.pdf>

<http://ailab.wsu.edu/subdue/papers/NobleKDD03.pdf>

Software

http://users.csc.tntech.edu/~weberle/gbad/thankyou.html

vast challenge

https://www.cs.umd.edu/hcil/varepository/VAST%20Challenge%202011/challenges/MC2%20-%20Computer%20Networking%20Operations/

**Servers to SSH to:**

onefish.csc.tntech.edu

twofish.csc.tntech.edu

Use TTU username & password

**Support:**

MyTech Helpdesk: 931-372-3975

Jared Jennings: 513-804-6771

**Folder System:**

Code: Where all the code that I write will be stored

Data Description: documents that gives descriptions of the datasets and the different values in each dataset

Gantt Chart Schedule – Gantt chart representation of a schedule for the research project

Lecture Folder – Contains PowerPoints of morning lectures

My Research Paper – where I will put the contents related to my research papers such as formatting guidelines, actual paper, images, graphs, and etc.

Related Research Paper – other research related to my research topic

Research papers will have numbers in front of their names so I can just use the number instead of writing the research paper name and author for citation purposes during the initial research process. The numbers increment by 1.

UMD Competition – guidelines, solutions, and other related info to the UMD Competition

Weekly PowerPoints – PowerPoints for my weekly presentation

Weekly Project Report – My weekly project reports

**Interesting things about the dataset**

IDS Log flagged the DOS attack at 11:43 while the firewall logged at 11:39. It took a while for the IDS log to pick up on the DOS attack

IDS Log only has 5 instances of DOS attack while the firewall log has multiple instances of DOS attacks

IDS Log has classification of Attempted Denial of Service which is an anomaly from "[Empty]"

Snort Rule File is 1:100000160:2 in IDS Log for all instances of DOS message with the same description text, "COMMUNITY SIP TCP/IP message flooding directed to SIP proxy" - in the graph we can just use the Snort Rule File as a node/edge value and use a dictionary to look up Snort Text Description.

Interesting thing is that the source IP/Port in the IDS log:

10.200.150.207:80

10.200.150.206:80

10.200.150.201:80

10.200.150.209:80

10.200.150.208:80

While the destionation IP/Port in the IDS log:

172.20.1.5:56760

172.20.1.5:56762

172.20.1.5:56763

172.20.1.5:56765

172.20.1.5:56766

Interesting thing is that the source IP/Port in the Firewall log (where x is differen values besides port 80) :

10.200.150.207:x

10.200.150.206:x

10.200.150.201:x

10.200.150.209:x

10.200.150.208:x

While the destionation IP/Port in the IDS log (Denial of service attach has the same destionation IP/Port but different source port as seen in the Firewall log):

172.20.1.5:80

**Files Need to Print:**