Peter Hogya

Executive Summary

The purpose of this project is to utilize Snort as an Intrusion Detection System (IDS) using an analytical data driven approach. An Intrusion Detection System monitors network activity and logs suspicious or harmful activity. This project does not attempt to implement an Intrusion Prevention System (IPS), which seeks to stop some of the detected suspicious or harmful activity. There are two general approaches to implementing an IDS, a signature-based detection system and an anomaly-based detection system. A signature-based detection system uses information about known attacks to create signatures for those attacks then compares incoming traffic against signatures to determine if there are any attacks. An anomaly-based detection system uses information about what normal network traffic is like and logs traffic that is abnormal. Both approaches are implemented in this project. Both approaches were also quite successful in properly identifying malicious traffic among normal traffic with success rates above 99% in the data analysis stage and nearly the same in the implementation stage for the signature-based detection system.

Specification

As stated previously, the goal of this project is to implement both types of IDSs, signature-based and anomaly-based, with some reasonable degree of accuracy in differentiating malicious and benign traffic. The first step in this process was finding pcap, packet capture, files that contained information about both different types of network attacks as well as of normal traffic. The specific sources for these data sets can be found in the ISSsource.pdf file.

The next step was to filter the features used later in the data analysis step from the pcap data sets and convert them into csv, comma-separated value, files. This was done using Wireshark. Further details about the specific features selected and why can be found below in the Methods and Techniques section.

Next the csv files needed to be preprocessed for use with data analysis tools. This was done using the Python programming language and a small program I wrote myself called ISSpreprocessing.py. More specific details provided below as well. Primarily the program trims data that would negatively impact performance and scaled all numeric values to between zero and one for equal weighting during the data analysis step. The data was also copied into two groups, one for the signature-based detection system where the specific attacks were labeled and one for the anomaly-based detection system where all attacks were labeled as abnormal.

Afterwards the files were modified into arff files. This just requires labeling of features and assigning sets to non-numeric features.

Once the data was preprocessed it was analyzed using the machine learning and predictive modeling suite, Weka. Specifically the J48 decision tree algorithm was used as I have a good deal of experience with decision tree algorithms and was able to troubleshoot more

easily. The data was classified with a 66% split between learning and testing data, as advised in the project specifications. Weka output decision trees for both the signature-based data set and the anomaly-based data set with correct classification rates above 99%. More specifics how this was achieved is detailed in the next section and the success rates are more thoroughly quantified in the results section.

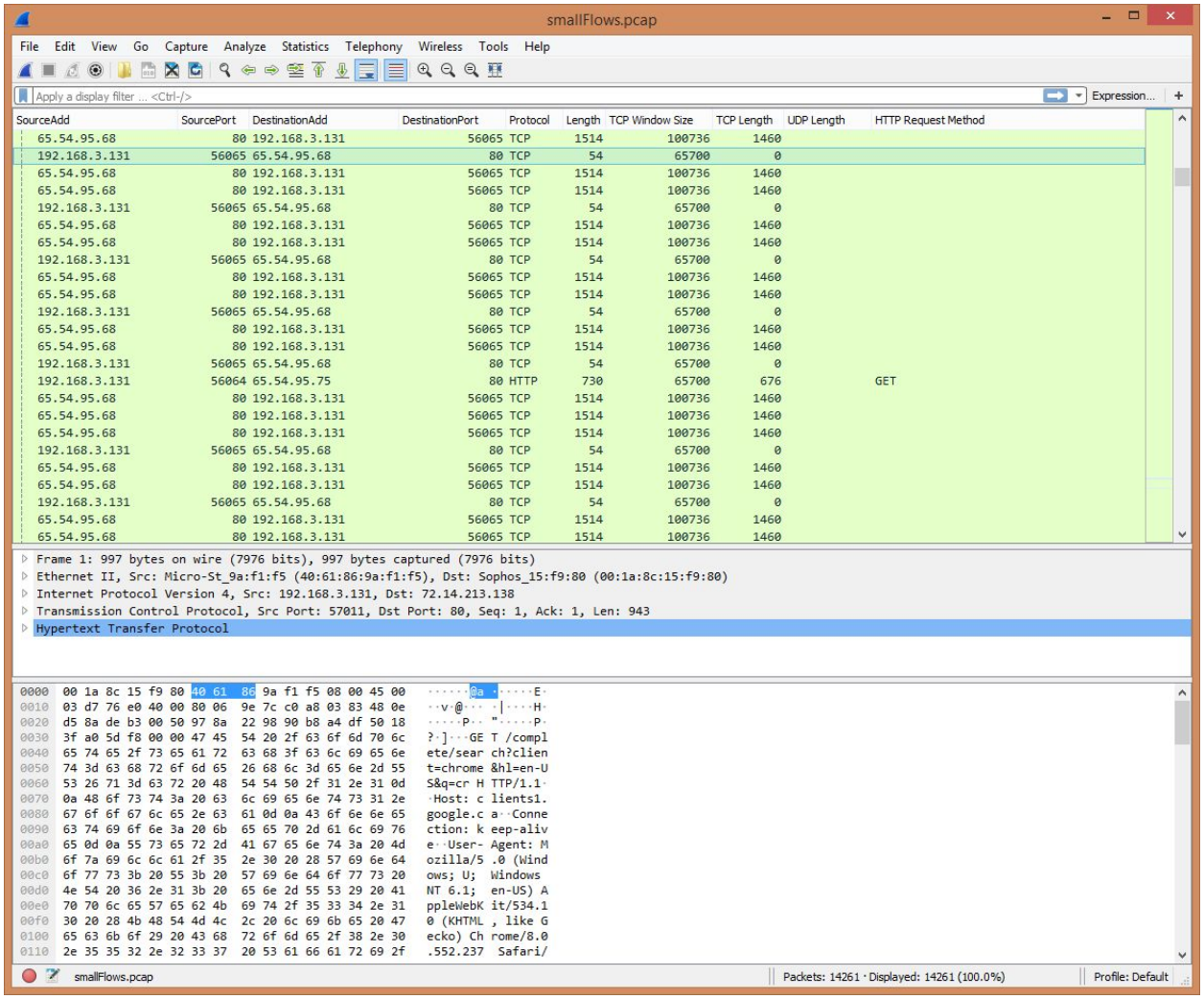
After acquiring useful decision trees from Weka the features in the trees were converted back into their original form partly with the help of some online tools and partly by hand. Then a list of general rules was determined using both the signature and anomaly based trees. The transcribed trees can be found in the ISStreetranscriptions.pdf file and the general rules can be found in the ISSrawrules.pdf file. More online tools were used alongside another Python program, ISSrulemaker.py, to convert the general rules into more specific rules that could be used in Snort. These rules are included in several different groupings in the rules folder. It includes a file with all the rules, a file with just the signature-based rules, a file with just the anomaly-based rules, and 5 files, one for each type of attack, labeled appropriately. Details on the specifics of these processes can be found in the next section.

Finally the specific rules were supplied to Snort and tested on the original pcap data. Practical success rates in Snort were similar to the theoretic success rates of the decision trees in Weka, despite some problems, and are analyzed in more detail in the results section.

Methods and Techniques

The pcap data files were filtered and converted into csv files using WireShark. Source IP, Destination IP, Source Port, Destination Port, and Protocol were selected because they provide the most information about the packet and were what the decision trees used exclusively. Packet Length, TCP Length, UDP Length, and TCP Window Size were selected as they provide wide ranges from which to differentiate traffic but were later scrapped due to incompatibility with Snort's rule formats. HTTP Request Method was selected as there are methods which are very clearly designated as unsafe and therefore provides a clear way to differentiate between some forms of suspicious traffic, however few methods were used across the data and this feature went unused in the decision trees.

Wireshark with selected data columns:



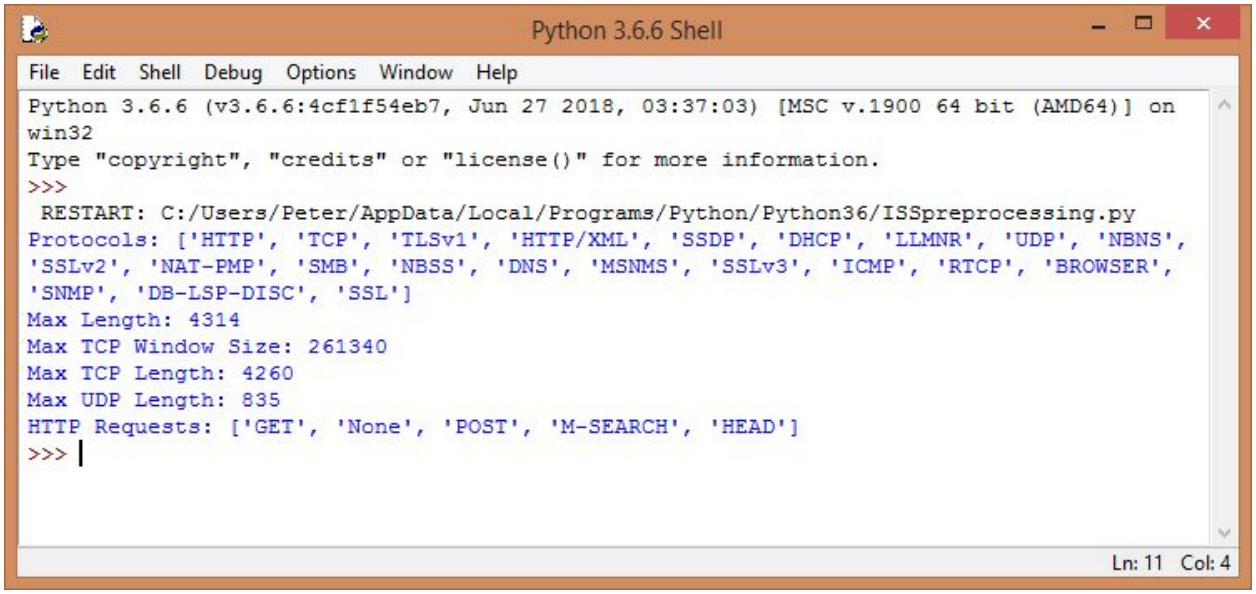
SourceAdd	SourcePort	DestinationAdd	DestinationPort	Protocol	Length	TCP Window Size	TCP Length	UDP Length	HTTP Request Method
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
192.168.3.131	56065	65.54.95.68	80	TCP	54	65700	0		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
192.168.3.131	56065	65.54.95.68	80	TCP	54	65700	0		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
192.168.3.131	56065	65.54.95.68	80	TCP	54	65700	0		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
192.168.3.131	56065	65.54.95.68	80	TCP	54	65700	0		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
192.168.3.131	56065	65.54.95.68	80	TCP	54	65700	0		
192.168.3.131	56064	65.54.95.75	80	HTTP	730	65700	676		GET
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
192.168.3.131	56065	65.54.95.68	80	TCP	54	65700	0		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
192.168.3.131	56065	65.54.95.68	80	TCP	54	65700	0		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		
65.54.95.68	80	192.168.3.131	56065	TCP	1514	100736	1460		

```
▷ Frame 1: 997 bytes on wire (7976 bits), 997 bytes captured (7976 bits)
▷ Ethernet II, Src: Micro-St_9a:f1:f5 (40:61:86:9a:f1:f5), Dst: Sophos_15:f9:80 (00:1a:8c:15:f9:80)
▷ Internet Protocol Version 4, Src: 192.168.3.131, Dst: 72.14.213.138
▷ Transmission Control Protocol, Src Port: 57011, Dst Port: 80, Seq: 1, Ack: 1, Len: 943
▷ Hypertext Transfer Protocol
```

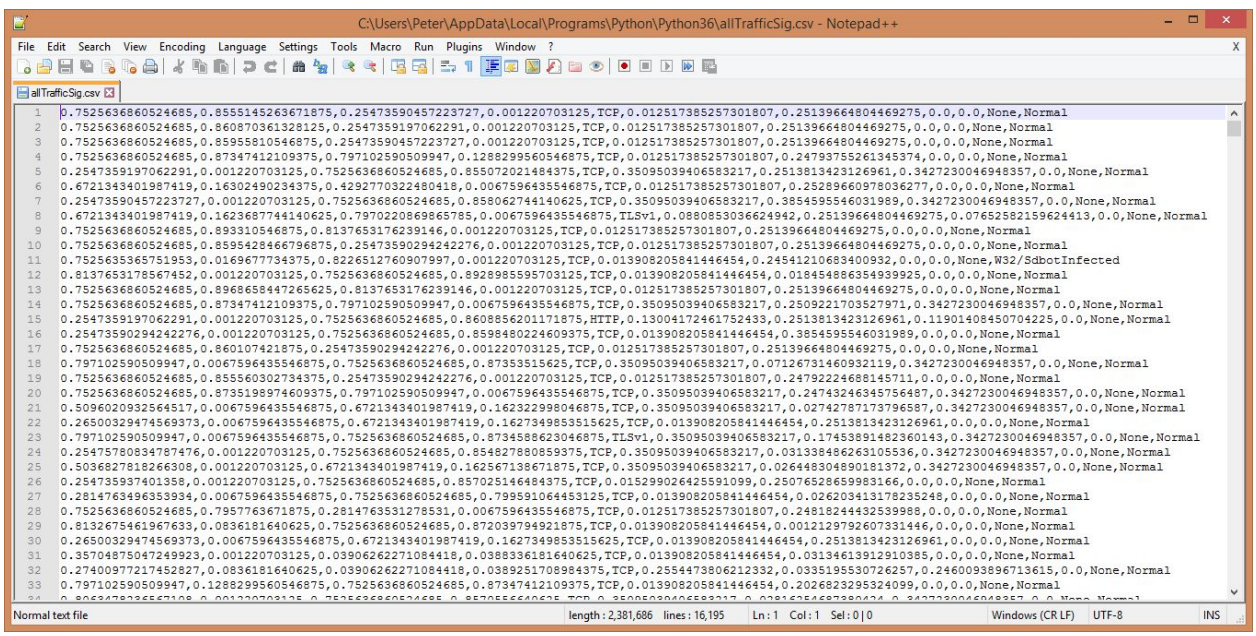
```
0000  00 1a 8c 15 f9 80 40 61  86 9a f1 f5 08 00 45 00   ······@a ······E·
0010  03 d7 76 e0 40 00 80 06  9e 7c c0 a8 03 83 48 0e   ··v·@··· ·|····H·
0020  d5 8a de b3 00 50 97 8a  22 98 90 b8 a4 df 50 18   ·····P·· "·····P·
0030  3f a0 5d f8 00 00 47 45  54 20 2f 63 6f 6d 70 6c   ?·]···GE T /compl
0040  65 74 65 2f 73 65 61 72  63 68 3f 63 6c 69 65 6e   ete/sear ch?clien
0050  74 3d 63 68 72 6f 6d 65  26 68 6c 3d 65 6e 2d 55   t=chrome &hl=en-U
0060  53 26 71 3d 63 72 20 48  54 54 50 2f 31 2e 31 0d   S&q=cr H TTP/1.1·
0070  0a 48 6f 73 74 3a 20 63  6c 69 65 6e 74 73 31 2e   ·Host: c lients1.
0080  67 6f 6f 67 6c 65 2e 63  61 0d 0a 43 6f 6e 6e 65   google.c a··Conne
0090  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
00a0  65 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   e··User- Agent: M
00b0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 57 69 6e 64   ozilla/5 .0 (Wind
00c0  6f 77 73 3b 20 55 3b 20  57 69 6e 64 6f 77 73 20   ows; U;  Windows 
00d0  4e 54 20 36 2e 31 3b 20  65 6e 2d 55 53 29 20 41   NT 6.1;  en-US) A
00e0  70 70 6c 65 57 65 62 4b  69 74 2f 35 33 34 2e 31   ppleWebK it/534.1
00f0  30 20 28 4b 48 54 4d 4c  2c 20 6c 69 6b 65 20 47   0 (KHTML , like G
0100  65 63 6b 6f 29 20 43 68  72 6f 6d 65 2f 38 2e 30   ecko) Ch rome/8.0
0110  2e 35 35 32 2e 32 33 37  20 53 61 66 61 72 69 2f   .552.237  Safari/
```

The csv files were then preprocessed using the ISSpreprocessing.py Python file. It removes 'ARF' protocol packets as their IP addresses are different. It also removes packets with empty source and/or destination ports. Any empty numeric fields, UDP Length,etc, are filled with a 0. Any empty HTTP Requests Methods are filled with a 'None' string. Then it converts IP addresses to integers and scales all numeric data from 0-1. The program outputs maximum values found for certain numeric fields for use in converting those fields back into their original form later. It also outputs all found classes for non-numeric fields. The new csv files are written by the program to the files in the csvs folder. The data is shuffled before it is written to the new files.

Program Output:

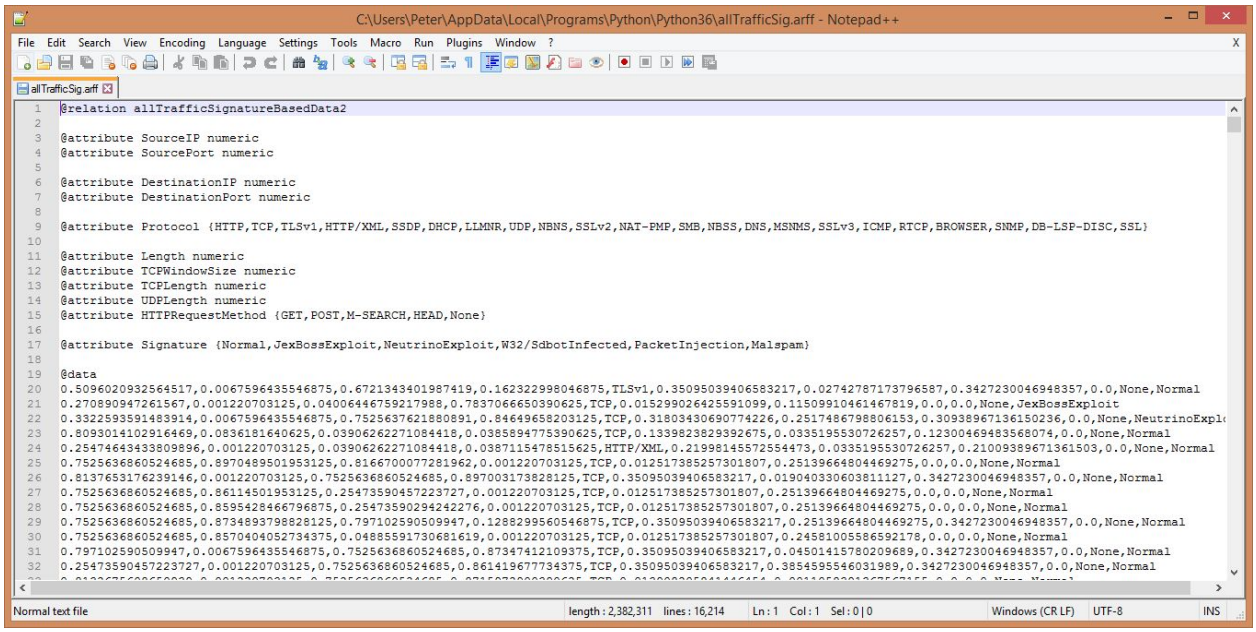


Sample of outputted csv files:



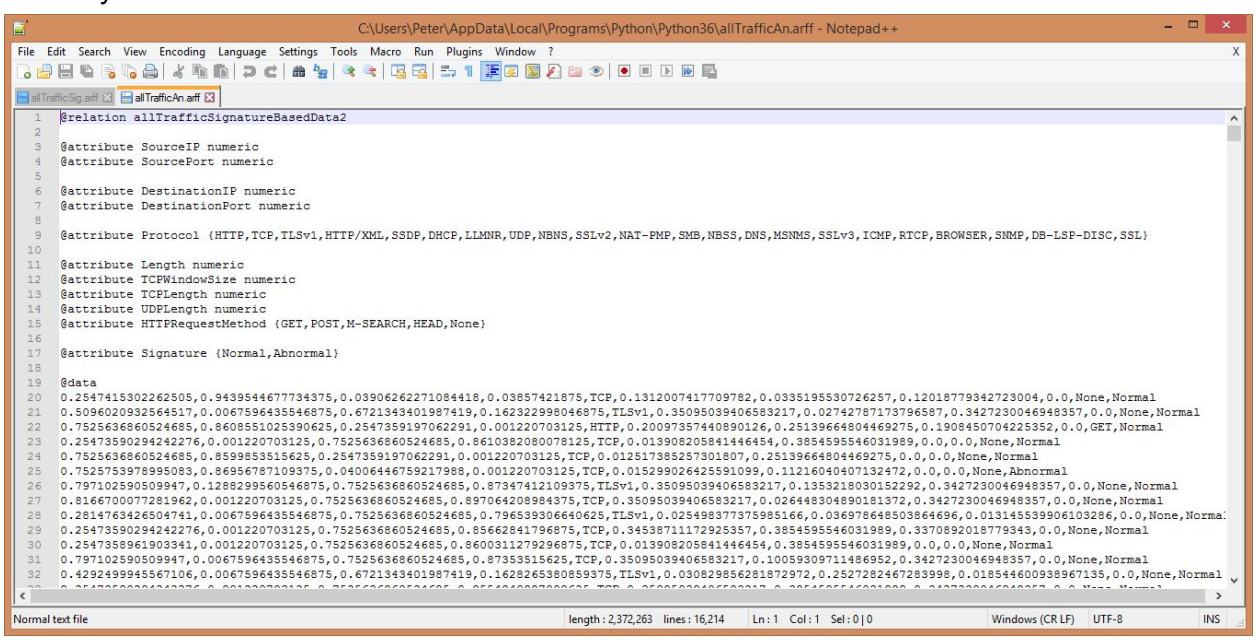
The csv files were then converted to arff files.

Signature arff file:




```
@relation allTrafficSignatureBasedData2

@attribute SourceIP numeric
@attribute SourcePort numeric

@attribute DestinationIP numeric
@attribute DestinationPort numeric

@attribute Protocol {HTTP,TCP,TLSv1,HTTP/XML,SSDP,DHCP,LLMNR,UDP,NBNS,SSLv2,NAT-PMP,SMB,NBSS,DNS,MSNMS,SSLv3,ICMP,RTCP,BROWSER,SNMP,DB-LSP-DISC,SSL}

@attribute Length numeric
@attribute TCPWindowSize numeric
@attribute TCPLength numeric
@attribute UDPLength numeric
@attribute HTTPRequestMethod {GET,POST,M-SEARCH,HEAD,None}

@attribute Signature {Normal,JexBossExploit,NeutrinoExploit,W32/SdbotInfected,PacketInjection,Malspam}

@data
0.5096020932564517,0.0067596435546875,0.6721343401987419,0.162322998046875,TLSv1,0.35095039406583217,0.02742787173796587,0.3427230046948357,0.0,None,Normal
0.270890947261567,0.001220703125,0.0400644675921798 8,0.7837066650390625,TCP,0.015299026425591099,0.11509910461467819,0.0,0.0,None,JexBossExploit
0.3322593591483914,0.0067596435546875,0.7525637621880891,0.84649658203125,TCP,0.31803430690774226,0.2517486798806153,0.30938967136150236,0.0,None,NeutrinoExpl
0.8093014102916469,0.0836181640625,0.03906262271084418,0.0385894775390625,TCP,0.1339823829392675,0.0335195530726257,0.12300469483568074,0.0,None,Normal
0.2547464343809896,0.001220703125,0.03906262271084418,0.0387115478515625,HTTP/XML,0.21998145572554473,0.0335195530726257,0.21009389671361503,0.0,None,Normal
0.7525636860524685,0.8970489501953125,0.8166700077281962,0.001220703125,TCP,0.012517385257301807,0.25139664804469275,0.0,0.0,None,Normal
0.8137653176239146,0.001220703125,0.7525636860524685,0.897003173828125,TCP,0.35095039406583217,0.01904033060381 1127,0.3427230046948357,0.0,None,Normal
0.7525636860524685,0.8611450195312 5,0.25473590457223727,0.001220703125,TCP,0.012517385257301807,0.25139664804469275,0.0,0.0,None,Normal
0.7525636860524685,0.8595428466796875,0.25473590294242276,0.001220703125,TCP,0.012517385257301807,0.25139664804469275,0.0,0.0,None,Normal
0.7525636860524685,0.8734893798828125,0.797102590509947,0.1288299560546875,TCP,0.35095039406583217,0.25139664804469275,0.3427230046948357,0.0,None,Normal
0.7525636860524685,0.8570404052734375,0.0488559173068 1619,0.001220703125,TCP,0.012517385257301807,0.24581005586592178,0.0,0.0,None,Normal
0.797102590509947,0.0067596435546875,0.7525636860524685,0.87347412109375,TCP,0.35095039406583217,0.04501415780209689,0.3427230046948357,0.0,None,Normal
0.25473590457223727,0.001220703125,0.7525636860524685,0.861419677734375,TCP,0.35095039406583217,0.3854595546031989,0.3427230046948357,0.0,None,Normal
```

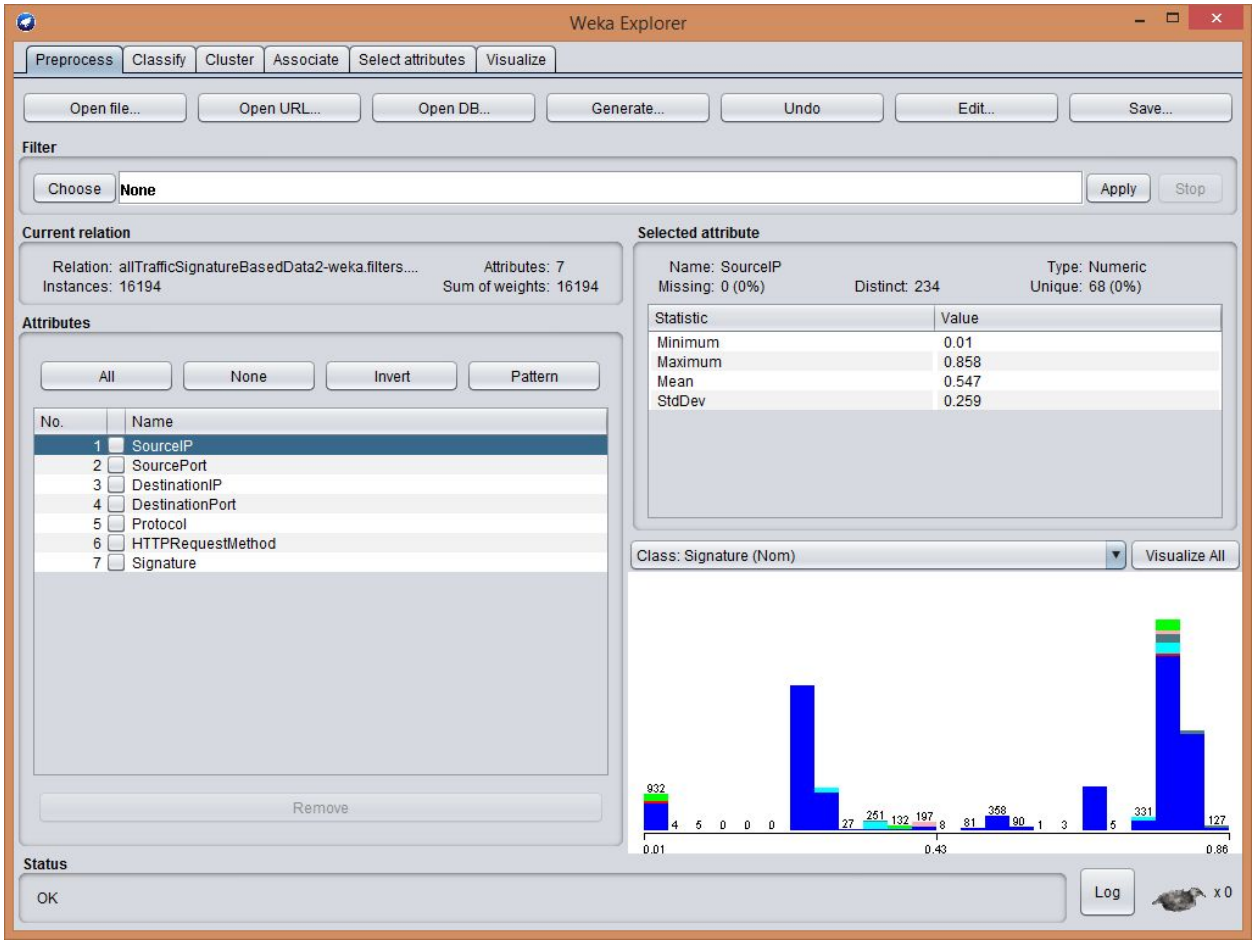
Anomaly arff file:




```
@relation allTrafficSignatureBasedData2

@attribute SourceIP numeric
@attribute SourcePort numeric

@attribute DestinationIP numeric
@attribute DestinationPort numeric

@attribute Protocol {HTTP,TCP,TLSv1,HTTP/XML,SSDP,DHCP,LLMNR,UDP,NBNS,SSLv2,NAT-PMP,SMB,NBSS,DNS,MSNMS,SSLv3,ICMP,RTCP,BROWSER,SNMP,DB-LSP-DISC,SSL}

@attribute Length numeric
@attribute TCPWindowSize numeric
@attribute TCPLength numeric
@attribute UDPLength numeric
@attribute HTTPRequestMethod {GET,POST,M-SEARCH,HEAD,None}

@attribute Signature {Normal,Abnormal}

@data
0.2547415302262505,0.9439544677734375,0.03906262271084418,0.03857421875,TCP,0.1312007417709782,0.0335195530726257,0.12018779342723004,0.0,None,Normal
0.5096020932564517,0.0067596435546875,0.6721343401987419,0.162322998046875,TLSv1,0.35095039406583217,0.02742787173796587,0.3427230046948357,0.0,None,Normal
0.7525636860524685,0.8608551025390625,0.2547359197062291,0.001220703125,HTTP,0.20097357440890126,0.25139664804469275,0.1908450704225352,0.0,GET,Normal
0.25473590294242276,0.001220703125,0.7525636860524685,0.861038208007812 5,TCP,0.013908205841446454,0.3854595546031989,0.0,0.0,None,Normal
0.7525636860524685,0.8599853515625,0.2547359197062291,0.001220703125,TCP,0.012517385257301807,0.25139664804469275,0.0,0.0,None,Normal
0.7525753978995083,0.8695678710937 5,0.04006446759217988,0.001220703125,TCP,0.015299026425591099,0.11216040407132472,0.0,0.0,None,Abnormal
0.797102590509947,0.1288299560546875,0.7525636860524685,0.87347412109375,TLSv1,0.35095039406583217,0.1353218030152292,0.3427230046948357,0.0,None,Normal
0.8166700077281962,0.001220703125,0.7525636860524685,0.897064208984375,TCP,0.35095039406583217,0.02644830489018 1372,0.3427230046948357,0.0,None,Normal
0.2814763426504741,0.0067596435546875,0.7525636860524685,0.796539306640625,TLSv1,0.02549837737598 5166,0.03697864850386 4696,0.013145539906103286,0.0,None,Normal
0.25473590294242276,0.001220703125,0.7525636860524685,0.8566284179687 5,TCP,0.3453871117292535 7,0.3854595546031989,0.3370892018779343,0.0,None,Normal
0.2547358961903341,0.001220703125,0.7525636860524685,0.860031127929687 5,TCP,0.013908205841446454,0.3854595546031989,0.0,0.0,None,Normal
0.797102590509947,0.0067596435546875,0.7525636860524685,0.87353515625,TCP,0.35095039406583217,0.1005930971148 6952,0.3427230046948357,0.0,None,Normal
0.4292499945567106,0.0067596435546875,0.6721343401987419,0.162826538085937 5,TLSv1,0.03082985628187 2972,0.2527282467283998,0.018544600938967135,0.0,None,Normal
```

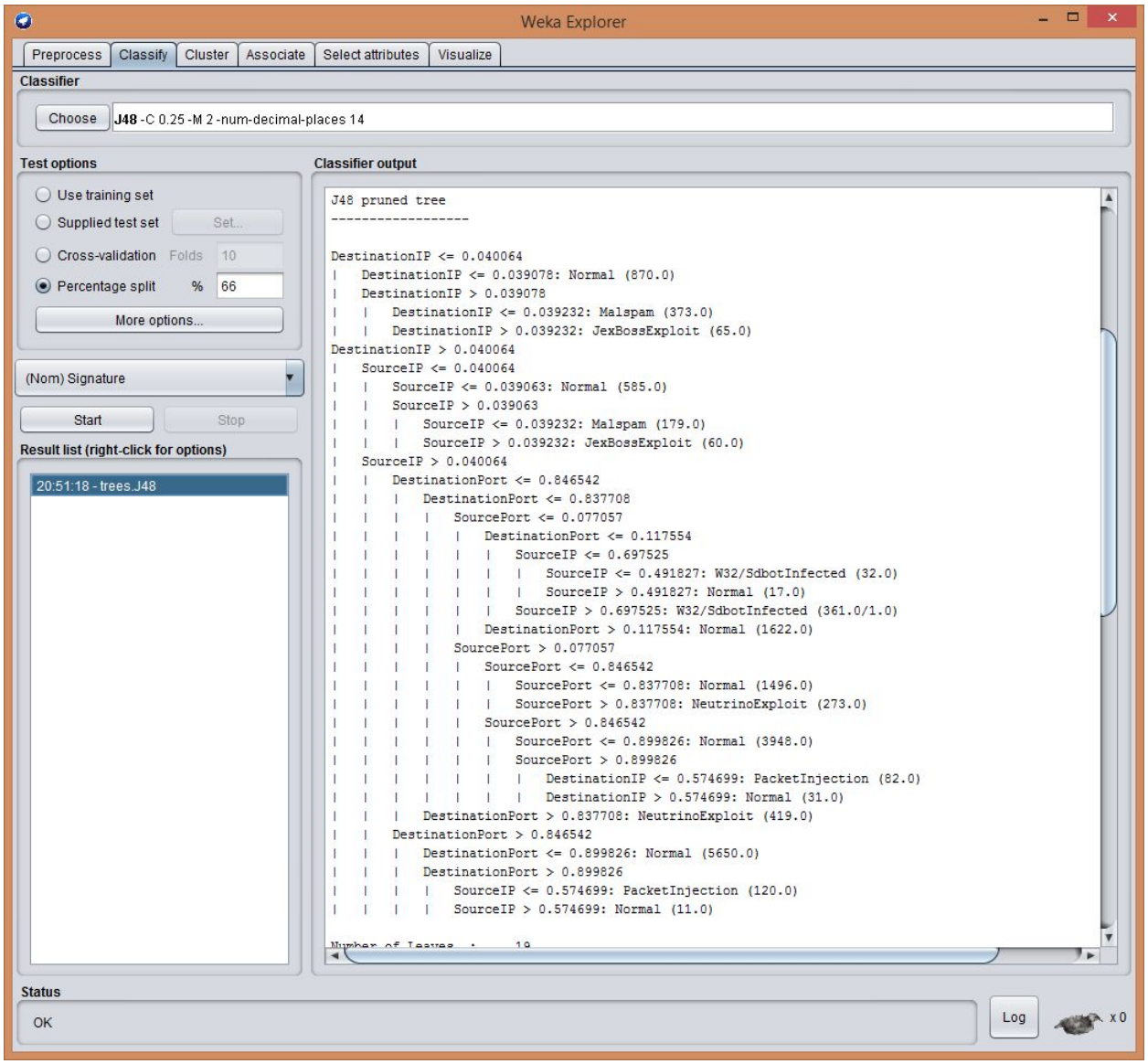
The arff files were then used in Weka to build the decision trees. The various length features were trimmed using Weka.

Weka with length features trimmed:

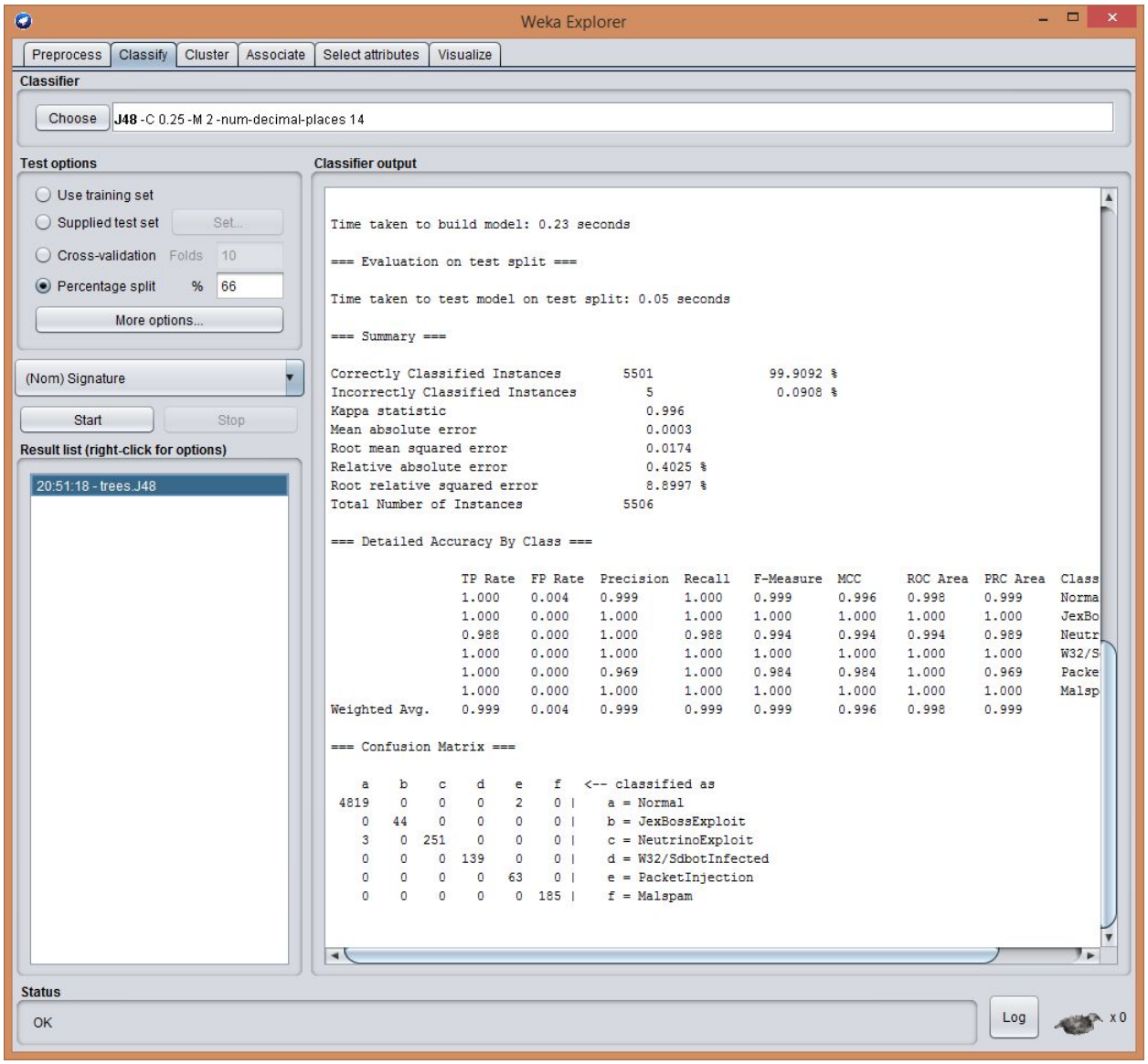


The J48 decision tree algorithm was then run on the data with the num-decimal-places flag set to 14 as integer IP addresses scaled from 0-1 are very small numbers. Some part of the differences between classification rates between the Weka trees and Snort can likely be attributed to rounding errors here. Note that these are not the actual trees used later, those are recorded in the ISStreetranscriptions.pdf file. An example of the anomaly-based tree is omitted as they tended to be much larger.

Weka decision tree output for signature-based data:



Weka classification rates and confusion matrix for signature-based tree:



The data in the trees was then converted by hand and with an online IP conversion tool back into their original values in the ISStreetranscriptions.pdf file. Then these new trees were converted into general rules by hand. These rules can be found in the ISSrawrules.pdf file. The general rules were then converted into Snort rules using a Python program, ISSrulemaker.py, and another online IP conversion tool. It outputs the rules directly once certain variables have been adjusted. These were then copied into several Snort rules file. These are separated several ways for testing purposes. There is a rules file for each attack, then a rules file for all signature-based attacks, then a rules file for anomaly-based detection, then a rules file for all the rules together. These can be found in the rules folder.

ISSrulemaker.py sample output:

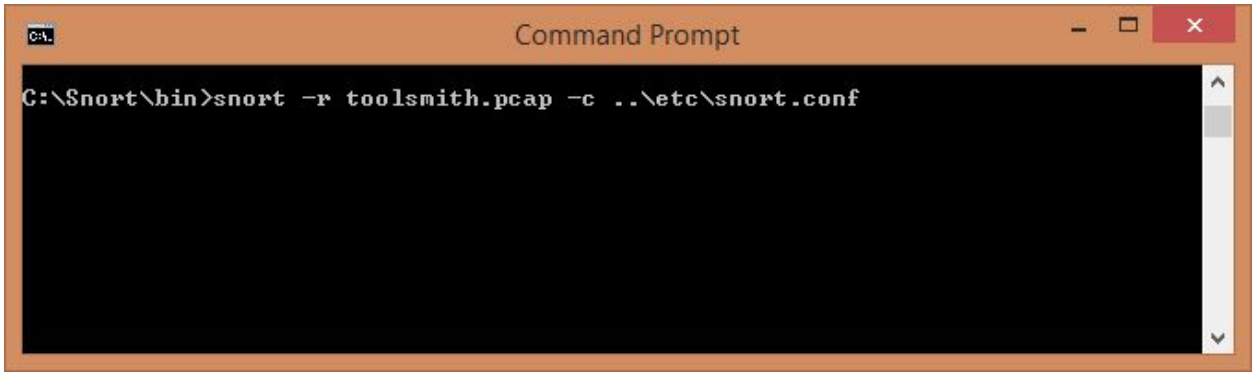
```
Python 3.6.6 Shell
File Edit Shell Debug Options Window Help
>>>
 RESTART: C:/Users/Peter/AppData/Local/Programs/Python/Python36/ISSrulemaker.py
alert tcp any any -> 192.168.8.199/32 55480: (msg: "Abnormal"; sid:1007873;)
alert tcp any any -> 192.168.8.200/29 55480: (msg: "Abnormal"; sid:1007874;)
alert tcp any any -> 192.168.8.208/28 55480: (msg: "Abnormal"; sid:1007875;)
alert tcp any any -> 192.168.8.224/27 55480: (msg: "Abnormal"; sid:1007876;)
alert tcp any any -> 192.168.9.0/24 55480: (msg: "Abnormal"; sid:1007877;)
alert tcp any any -> 192.168.10.0/23 55480: (msg: "Abnormal"; sid:1007878;)
alert tcp any any -> 192.168.12.0/22 55480: (msg: "Abnormal"; sid:1007879;)
alert tcp any any -> 192.168.16.0/20 55480: (msg: "Abnormal"; sid:1007880;)
alert tcp any any -> 192.168.32.0/19 55480: (msg: "Abnormal"; sid:1007881;)
alert tcp any any -> 192.168.64.0/18 55480: (msg: "Abnormal"; sid:1007882;)
alert tcp any any -> 192.168.128.0/17 55480: (msg: "Abnormal"; sid:1007883;)
alert tcp any any -> 192.169.0.0/16 55480: (msg: "Abnormal"; sid:1007884;)
alert tcp any any -> 192.170.0.0/15 55480: (msg: "Abnormal"; sid:1007885;)
alert tcp any any -> 192.172.0.0/14 55480: (msg: "Abnormal"; sid:1007886;)
alert tcp any any -> 192.176.0.0/12 55480: (msg: "Abnormal"; sid:1007887;)
alert tcp any any -> 192.192.0.0/10 55480: (msg: "Abnormal"; sid:1007888;)
alert tcp any any -> 193.0.0.0/8 55480: (msg: "Abnormal"; sid:1007889;)
alert tcp any any -> 194.0.0.0/7 55480: (msg: "Abnormal"; sid:1007890;)
alert tcp any any -> 196.0.0.0/6 55480: (msg: "Abnormal"; sid:1007891;)
alert tcp any any -> 200.0.0.0/5 55480: (msg: "Abnormal"; sid:1007892;)
alert tcp any any -> 208.0.0.0/4 55480: (msg: "Abnormal"; sid:1007893;)
alert tcp any any -> 224.0.0.0/3 55480: (msg: "Abnormal"; sid:1007894;)
>>>
Ln: 12028  Col: 75
```

Sample of rules file:

```
C:\Snort\rules\signature.rules - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
allTrafficSig.arff | allTrafficAn.arff | signature.rules
# Malspam Rule Set 1
alert tcp any any -> 10.1.4.13/30 any (msg: "Malspam"; sid:1000002;)
alert tcp any any -> 10.1.4.16/28 any (msg: "Malspam"; sid:1000003;)
alert tcp any any -> 10.1.4.32/27 any (msg: "Malspam"; sid:1000004;)
alert tcp any any -> 10.1.4.128/25 any (msg: "Malspam"; sid:1000005;)
alert tcp any any -> 10.1.5.0/24 any (msg: "Malspam"; sid:1000006;)
alert tcp any any -> 10.1.6.0/23 any (msg: "Malspam"; sid:1000007;)
alert tcp any any -> 10.1.8.0/21 any (msg: "Malspam"; sid:1000008;)
alert tcp any any -> 10.1.16.0/20 any (msg: "Malspam"; sid:1000009;)
alert tcp any any -> 10.1.32.0/19 any (msg: "Malspam"; sid:1000010;)
alert tcp any any -> 10.1.64.0/18 any (msg: "Malspam"; sid:1000011;)
alert tcp any any -> 10.1.128.0/17 any (msg: "Malspam"; sid:1000012;)
alert tcp any any -> 10.2.0.0/15 any (msg: "Malspam"; sid:1000013;)
alert tcp any any -> 10.4.0.0/14 any (msg: "Malspam"; sid:1000014;)
alert tcp any any -> 10.8.0.0/15 any (msg: "Malspam"; sid:1000015;)
alert tcp any any -> 10.10.0.0/16 any (msg: "Malspam"; sid:1000016;)
alert tcp any any -> 10.11.0.0/20 any (msg: "Malspam"; sid:1000017;)
alert tcp any any -> 10.11.16.0/21 any (msg: "Malspam"; sid:1000018;)
alert tcp any any -> 10.11.24.0/23 any (msg: "Malspam"; sid:1000019;)
alert tcp any any -> 10.11.26.0/24 any (msg: "Malspam"; sid:1000020;)
alert tcp any any -> 10.11.27.0/25 any (msg: "Malspam"; sid:1000021;)
alert tcp any any -> 10.11.27.128/27 any (msg: "Malspam"; sid:1000022;)
alert tcp any any -> 10.11.27.160/28 any (msg: "Malspam"; sid:1000023;)
alert tcp any any -> 10.11.27.176/29 any (msg: "Malspam"; sid:1000024;)
alert tcp any any -> 10.11.27.184/30 any (msg: "Malspam"; sid:1000025;)
alert tcp any any -> 10.11.27.188/31 any (msg: "Malspam"; sid:1000026;)

# JexBossExploit Rule Set 1
alert tcp any any -> 10.11.27.190/32 any (msg: "JexBossExploit"; sid:1000027;)
alert tcp any any -> 10.11.27.190/31 any (msg: "JexBossExploit"; sid:1000028;)
alert tcp any any -> 10.11.27.192/26 any (msg: "JexBossExploit"; sid:1000029;)
alert tcp any any -> 10.11.28.0/22 any (msg: "JexBossExploit"; sid:1000030;)
alert tcp any any -> 10.11.32.0/19 any (msg: "JexBossExploit"; sid:1000031;)
Normal text file | length : 877,544  lines : 9,498 | Ln : 1  Col : 1  Sel : 0 | 0 | Windows (CR LF) | UTF-8 | INS
```

The rules files were then added to the snort.conf file in Snort, while disabling all other rules. Then the files were tested by running the pcap files directly through Snort.

Snort command line to test a pcap file:



Snort result of testing above pcap file:

Command Prompt

```
==============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:          425 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          425 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:           18 (  4.235%)
        TCP:          407 ( 95.765%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:           33 (  7.765%)
     S5 G 2:            0 (  0.000%)
      Total:          425
==============================================================================
Action Stats:
     Alerts:          392 ( 92.235%)
     Logged:          392 ( 92.235%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:          101
Verdicts:
      Allow:          392 (100.000%)
```

Testing

Testing was done in two parts. First the decision trees were automatically tested in Weka using the 66% split. This provided a theoretical high of classification efficacy. Second the rules files were tested using Snort. This provided an applied classification efficacy. Note that any protocols aside from TCP and UDP were ignored in the evaluation of Snort.

More specifically the equations supplied in class from https://en.wikipedia.org/wiki/Precision_and_recall were used to evaluate the two different steps in the project. Data from the output of both Weka and Snort are listed in the Results section for reference to the values used in the equations.

Results

$$precision = \frac{TP}{TP+FP}$$
$$recall = \frac{TP}{TP+FN}$$
$$accuracy = \frac{TP+TN}{ALL}$$

For Weka signature-based:

```
=== Confusion Matrix ===

    a    b    c    d    e    f   <-- classified as
 4819    0    0    0    2    0 |    a = Normal
    0   44    0    0    0    0 |    b = JexBossExploit
    3    0  251    0    0    0 |    c = NeutrinoExploit
    0    0    0  139    0    0 |    d = W32/SdbotInfected
    0    0    0    0   63    0 |    e = PacketInjection
    0    0    0    0    0  185 |    f = Malspam
```

$$precision = \frac{682}{682+2} = 0.997$$
$$recall = \frac{682}{682+3} = 0.996$$
$$accuracy = \frac{682+4819}{682+4819+2+3} = 0.999$$

For Weka anomaly-based:

```
=== Confusion Matrix ===

    a    b   <-- classified as
 4831    2 |    a = Normal
    1  672 |    b = Abnormal
```

$$precision = \frac{672}{672+2} = 0.997$$
$$recall = \frac{672}{672+1} = 0.999$$
$$accuracy = \frac{672+4831}{672+4831+1+2} = 0.999$$

For Snort signature-based rules using allTraffic.pcap:

```
Command Prompt
===============================================================================
Run time for packet processing was 9.153000 seconds
Snort processed 16720 packets.
Snort ran for 0 days 0 hours 0 minutes 9 seconds
   Pkts/sec:         1857
===============================================================================
Packet I/O Totals:
   Received:        16720
   Analyzed:        16720 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:        16775 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:        16751 ( 99.857%)
       Frag:            0 (  0.000%)
       ICMP:           34 (  0.203%)
        UDP:          527 (  3.142%)
        TCP:        16190 ( 96.513%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:           24 (  0.143%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:          119 (  0.709%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:           50 (  0.298%)
     S5 G 2:            5 (  0.030%)
      Total:        16775
===============================================================================
Action Stats:
     Alerts:         2332 ( 13.902%)
     Logged:         2332 ( 13.902%)
     Passed:            0 (  0.000%)
Limits:
```

For Snort signature-based rules using smallflows.pcap (normal traffic):

```
Command Prompt
===============================================================================
Run time for packet processing was 7.652000 seconds
Snort processed 14261 packets.
Snort ran for 0 days 0 hours 0 minutes 7 seconds
   Pkts/sec:         2037
===============================================================================
Packet I/O Totals:
   Received:        14261
   Analyzed:        14261 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:        14277 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:        14259 ( 99.874%)
       Frag:            0 (  0.000%)
       ICMP:           34 (  0.238%)
        UDP:          501 (  3.509%)
        TCP:        13724 ( 96.127%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:           18 (  0.126%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:           12 (  0.084%)
     S5 G 2:            4 (  0.028%)
      Total:        14277
===============================================================================
Action Stats:
     Alerts:            1 (  0.007%)
     Logged:            1 (  0.007%)
     Passed:            0 (  0.000%)
Limits:
```

For Snort signature-based rules using toolsmith.pcap (W32/Sdbot Infected):

```
Command Prompt
===============================================================================
Run time for packet processing was 0.344000 seconds
Snort processed 392 packets.
Snort ran for 0 days 0 hours 0 minutes 0 seconds
   Pkts/sec:           392
===============================================================================
Packet I/O Totals:
   Received:           392
   Analyzed:           392 (100.000%)
    Dropped:             0 (  0.000%)
   Filtered:             0 (  0.000%)
Outstanding:             0 (  0.000%)
   Injected:             0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:           425 (100.000%)
       VLAN:             0 (  0.000%)
        IP4:           425 (100.000%)
       Frag:             0 (  0.000%)
       ICMP:             0 (  0.000%)
        UDP:            18 (  4.235%)
        TCP:           407 ( 95.765%)
        IP6:             0 (  0.000%)
    IP6 Ext:             0 (  0.000%)
   IP6 Opts:             0 (  0.000%)
      Frag6:             0 (  0.000%)
      ICMP6:             0 (  0.000%)
       UDP6:             0 (  0.000%)
       TCP6:             0 (  0.000%)
     Teredo:             0 (  0.000%)
    ICMP-IP:             0 (  0.000%)
      EAPOL:             0 (  0.000%)
    IP4/IP4:             0 (  0.000%)
    IP4/IP6:             0 (  0.000%)
    IP6/IP4:             0 (  0.000%)
    IP6/IP6:             0 (  0.000%)
        GRE:             0 (  0.000%)
    GRE Eth:             0 (  0.000%)
   GRE VLAN:             0 (  0.000%)
    GRE IP4:             0 (  0.000%)
    GRE IP6:             0 (  0.000%)
GRE IP6 Ext:             0 (  0.000%)
   GRE PPTP:             0 (  0.000%)
    GRE ARP:             0 (  0.000%)
    GRE IPX:             0 (  0.000%)
   GRE Loop:             0 (  0.000%)
       MPLS:             0 (  0.000%)
        ARP:             0 (  0.000%)
        IPX:             0 (  0.000%)
   Eth Loop:             0 (  0.000%)
   Eth Disc:             0 (  0.000%)
   IP4 Disc:             0 (  0.000%)
   IP6 Disc:             0 (  0.000%)
   TCP Disc:             0 (  0.000%)
   UDP Disc:             0 (  0.000%)
  ICMP Disc:             0 (  0.000%)
All Discard:             0 (  0.000%)
      Other:             0 (  0.000%)
Bad Chk Sum:             0 (  0.000%)
    Bad TTL:             0 (  0.000%)
     S5 G 1:            33 (  7.765%)
     S5 G 2:             0 (  0.000%)
      Total:           425
===============================================================================
Action Stats:
     Alerts:           392 ( 92.235%)
     Logged:           392 ( 92.235%)
     Passed:             0 (  0.000%)
Limits:
```

For Snort signature-based rules using hao123-com_packet-injection.pcap (Packet Injection):

```
Command Prompt
Snort ran for 0 days 0 hours 0 minutes 0 seconds
   Pkts/sec:          202
==============================================================================
Packet I/O Totals:
   Received:          202
   Analyzed:          202 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
==============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:            0 (  0.000%)
       VLAN:            0 (  0.000%)
        IP4:          202 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            0 (  0.000%)
        TCP:          202 (100.000%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
     Bad TTL:            0 (  0.000%)
      S5 G 1:            0 (  0.000%)
      S5 G 2:            0 (  0.000%)
       Total:          202
==============================================================================
Action Stats:
     Alerts:          202 (100.000%)
     Logged:          202 (100.000%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
```

For Snort signature-based rules using jexboss_attack_v6_victim_vantage.pcap (JexBoss Exploit):

```
Command Prompt
Snort ran for 0 days 0 hours 0 minutes 0 seconds
   Pkts/sec:          131
==================================================================================
Packet I/O Totals:
   Received:          131
   Analyzed:          131 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
==================================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:          131 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          125 ( 95.420%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            2 (  1.527%)
        TCP:          123 ( 93.893%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            6 (  4.580%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:          119 ( 90.840%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            0 (  0.000%)
     S5 G 2:            0 (  0.000%)
      Total:          131
==================================================================================
Action Stats:
     Alerts:            0 (  0.000%)
     Logged:            0 (  0.000%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
```

For Snort signature-based rules using 2016-08-16-Neutrino-EK.pcap (Neutrino Exploit):

```
Command Prompt
===============================================================================
Run time for packet processing was 0.484000 seconds
Snort processed 692 packets.
Snort ran for 0 days 0 hours 0 minutes 0 seconds
   Pkts/sec:          692
===============================================================================
Packet I/O Totals:
   Received:          692
   Analyzed:          692 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:          696 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          696 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            0 (  0.000%)
        TCP:          696 (100.000%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            3 (  0.431%)
     S5 G 2:            1 (  0.144%)
      Total:          696
===============================================================================
Action Stats:
     Alerts:          694 ( 99.713%)
     Logged:          694 ( 99.713%)
     Passed:            0 (  0.000%)
Limits:
```

For Snort signature-based rules using 2017-11-29-Emotet-malspam-2nd-run.pcap (malspam):

```
Command Prompt
Snort ran for 0 days 0 hours 0 minutes 0 seconds
   Pkts/sec:          552
===============================================================================
Packet I/O Totals:
   Received:          552
   Analyzed:          552 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:          554 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          554 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            6 (  1.083%)
        TCP:          548 ( 98.917%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
     Bad TTL:            0 (  0.000%)
      S5 G 1:            2 (  0.361%)
      S5 G 2:            0 (  0.000%)
       Total:          554
===============================================================================
Action Stats:
     Alerts:          553 ( 99.819%)
     Logged:          553 ( 99.819%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
```

Snort signature-based calculations:

$$TP = 553 + 694 + 0 + 202 + 392 = 1841$$
$$FP = 1$$
$$TN = 14277$$
$$FN = 1 + 2 + 131 + 0 + 33 = 167$$

$$precision = \frac{1841}{1841+1} = 0.999$$
$$recall = \frac{1841}{1841+167} 0.917$$
$$accuracy = \frac{1841+14277}{1841+1+14277+167} = \frac{16118}{16286} = 0.990$$

For Snort anomaly-based rules using allTraffic.pcap:

```
Command Prompt
===============================================================================
Run time for packet processing was 5.487000 seconds
Snort processed 16720 packets.
Snort ran for 0 days 0 hours 0 minutes 5 seconds
   Pkts/sec:         3344
===============================================================================
Packet I/O Totals:
   Received:        16720
   Analyzed:        16720 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:        16775 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:        16751 ( 99.857%)
       Frag:            0 (  0.000%)
       ICMP:           34 (  0.203%)
        UDP:          527 (  3.142%)
        TCP:        16190 ( 96.513%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:           24 (  0.143%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:          119 (  0.709%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:           50 (  0.298%)
     S5 G 2:            5 (  0.030%)
      Total:        16775
===============================================================================
Action Stats:
     Alerts:         3915 ( 23.338%)
     Logged:         3915 ( 23.338%)
     Passed:            0 (  0.000%)
Limits:
```

For Snort anomaly-based rules using smallflows.pcap (normal traffic):

```
Command Prompt
===============================================================================
Run time for packet processing was 4.594000 seconds
Snort processed 14261 packets.
Snort ran for 0 days 0 hours 0 minutes 4 seconds
   Pkts/sec:         3565
===============================================================================
Packet I/O Totals:
   Received:        14261
   Analyzed:        14261 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:        14277 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:        14259 ( 99.874%)
       Frag:            0 (  0.000%)
       ICMP:           34 (  0.238%)
        UDP:          501 (  3.509%)
        TCP:        13724 ( 96.127%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:           18 (  0.126%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:           12 (  0.084%)
     S5 G 2:            4 (  0.028%)
      Total:        14277
===============================================================================
Action Stats:
     Alerts:           65 (  0.455%)
     Logged:           65 (  0.455%)
     Passed:            0 (  0.000%)
Limits:
```

For Snort anomaly-based rules using 2016-08-16-Neutrino-EK.pcap (Neutrino Exploit):

```
Command Prompt
Snort ran for 0 days 0 hours 0 minutes 0 seconds
   Pkts/sec:          692
==========================================================================
Packet I/O Totals:
   Received:          692
   Analyzed:          692 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
==========================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:          696 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          696 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            0 (  0.000%)
        TCP:          696 (100.000%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
     Bad TTL:            0 (  0.000%)
      S5 G 1:            3 (  0.431%)
      S5 G 2:            1 (  0.144%)
       Total:          696
==========================================================================
Action Stats:
     Alerts:          967 (138.937%)
     Logged:          967 (138.937%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
```

For Snort anomaly-based rules using 2017-11-29-Emotet-malspam-2nd-run.pcap (malspam):

```
Command Prompt
Snort ran for 0 days 0 hours 0 minutes 0 seconds
   Pkts/sec:          552
===============================================================================
Packet I/O Totals:
   Received:          552
   Analyzed:          552 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:          554 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          554 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            6 (  1.083%)
        TCP:          548 ( 98.917%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
     Bad TTL:            0 (  0.000%)
      S5 G 1:            2 (  0.361%)
      S5 G 2:            0 (  0.000%)
       Total:          554
===============================================================================
Action Stats:
     Alerts:          551 ( 99.458%)
     Logged:          551 ( 99.458%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
```

For Snort anomaly-based rules using hao123-com_packet-injection.pcap (Packet Injection):

```
Snort ran for 0 days 0 hours 0 minutes 0 seconds
   Pkts/sec:          202
==============================================================================
Packet I/O Totals:
   Received:          202
   Analyzed:          202 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
==============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:            0 (  0.000%)
       VLAN:            0 (  0.000%)
        IP4:          202 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            0 (  0.000%)
        TCP:          202 (100.000%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
     Bad TTL:            0 (  0.000%)
      S5 G 1:            0 (  0.000%)
      S5 G 2:            0 (  0.000%)
       Total:          202
==============================================================================
Action Stats:
     Alerts:          404 (200.000%)
     Logged:          404 (200.000%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
```

For Snort anomaly-based rules using jexboss_attack_v6_victim_vantage.pcap (JexBoss Exploit):

```
Command Prompt
Snort ran for 0 days 0 hours 0 minutes 0 seconds
   Pkts/sec:          131
==================================================================================
Packet I/O Totals:
   Received:          131
   Analyzed:          131 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
==================================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:          131 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          125 ( 95.420%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            2 (  1.527%)
        TCP:          123 ( 93.893%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            6 (  4.580%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:          119 ( 90.840%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            0 (  0.000%)
     S5 G 2:            0 (  0.000%)
      Total:          131
==================================================================================
Action Stats:
     Alerts:            5 (  3.817%)
     Logged:            5 (  3.817%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
```

For Snort anomaly-based rules using toolsmith.pcap (W32/Sdbot Infected):

```
Command Prompt

Snort ran for 0 days 0 hours 0 minutes 0 seconds
   Pkts/sec:          392
==============================================================================
Packet I/O Totals:
   Received:          392
   Analyzed:          392 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
==============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:          425 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:          425 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:           18 (  4.235%)
        TCP:          407 ( 95.765%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:            0 (  0.000%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            0 (  0.000%)
Bad Chk Sum:            0 (  0.000%)
     Bad TTL:            0 (  0.000%)
      S5 G 1:           33 (  7.765%)
      S5 G 2:            0 (  0.000%)
       Total:          425
==============================================================================
Action Stats:
     Alerts:         1362 (320.471%)
     Logged:         1362 (320.471%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
```

There were some problems with running the rules through Snort. The signature-based rules would not detect any of the JexBoss Exploit pcap data. This skewed results to a degree however despite this the actual measurements remained fairly high as the JexBoss Exploit pcap data was relatively small compared to the whole data set and the rules performed very well on the rest of the data.

The efficacy of the anomaly-based rules are somewhat unclear as there are packets that trigger multiple alerts. This factor does not fit into the performance equations and also masks the actual performance as a 100% alert rate could simply mean one packet triggered as many alerts as there are packets in total.

Another problem was the significant reliance on IP addresses to differentiate between malicious and benign traffic. Mapping the entire IP address space to establish neighborhoods of credibility is a novel idea but is computationally intensive, especially with the address space of IPv6. The number of rules to cover a particular IP space is quite large, however this could be resolved fairly easily if Snort had a comparison operator for IP addresses. For some reason comparison operators only exist for ports. This is also why the length features were dropped as their usage would be very difficult with Snort. I considered using Suricata at one point as well but it also lacked comparison operators for many features.

Despite the numerous problems the results from the Weka trees and the Snort signature-based rule set both demonstrated very accurate detection rates, the latter of which could be significantly improved with a greater understanding of Snort.