Project 1: IDS Classifier Creation

Derrick Kempster
Department of Computer Science
Golisano College of Computing and Information Sciences
Rochester Institute of Technology
Rochester, NY 14586
dk9977@rit.edu

***Abstract*—An IDS is an important piece of software in the security of many computer systems. This project is to create the classifiers for a misuse IDS and anomaly IDS. To do this, Weka was employed for its ability to preprocess, classify, and analyze data. The provided network traffic data was preprocessed into training and test sets. A random forest classifier was created for each of the training sets. Running the test sets through the misuse and anomaly classifiers showed accuracies of 99.9773% and 99.9891%, respectively. Thus, Weka has shown to be quite a useful tool in classifier creation.**

***Keywords*— IDS, misuse, anomaly, Weka, classifier, random forest**

I. Specification

An IDS – intrusion detection system – is a piece of security software that monitors the traffic on a computer system. It is intended to detect and alert about suspicious activity from the network. The goal of this project is to create classifiers for a misuse IDS and an anomaly IDS. A misuse IDS focuses on identifying the network activity the attack it represents or normal. An anomaly IDS doesn't identify by signature, but instead classifies activity as normal or anomalous. To achieve IDS creation, an artificial intelligence program called Weka – short for the Waikato Environment for Knowledge Analysis – was employed. The tool assists with data preprocessing, classification, and analysis. The data used by an IDS consists of all available information in connections to a system. The information from a single connection composes a single record.

II. Methods and Techniques

The data of choice was provided by Professor Leonid Reznik. It was already normalized and put in separate files by the known associated attack. In order to change the data to a format acceptable by Weka, two programs were written: one for a misuse IDS and another for an anomaly IDS. In each, all of the provided files were combined into one Attribute-Relation File Format (.arff) file and each instance gained a "class" attribute. To discover misuse, this new attribute is the type of attack or "Normal" for normal behavior. To discover anomalies, it is "Normal" for normal behavior or "Anomaly" for any attack. There is a total of 823367 instances in each of these files. Then, this data was divided into training and testing sets. In the "Preprocess" section of the Weka Explorer, a filter of "Resample –S 45 –Z 70.0 –no-replacement" was applied to create and save a 70% training set (576356 instances). By undoing that filter, adding "-V", and applying the new filter, a 30% testing set (247011 instances) was created and then saved.

III. Implementation

In the "Preprocess" section of the Weka Explorer, the training set was loaded. Then in the "Classify" section, a classifier was trained and tested using a supplied test set – the one created before. Using the settings "RandomForest –P 100 –I 100 –num-slots 1 –K 0 –M 1.0 –V 0.001 –S 45 –depth 100", a random forest of 100 trees of maximum 100 depth was created. Table I shows the running time to build the random forest classifier model.

IV. Tests

After the model was constructed, the test set immediately ran. Each of the instances in the test set were run through the classifier to try to determine its identity. Table I shows the time to test each model.

V. Results

Table II shows the overall accuracy of each classifier. Table III shows the results of the anomaly IDS testing. Table IV shows the same for misuse IDS testing. In the latter two tables, "Class Acc. (%)" represents the portion of instances of that type which have been classified correctly, and "Determination Acc. (%)" represents the portion of instances of that classification which are actually of that type. Both classifiers have shown to be quite good, with accuracies very near to 100%. The anomaly classifier results of Table III seem to be good due to the small number of classes available. As can be seen in the misuse classifier results of Table IV, the attacks "Imap" and "MultiHop" had no records in the test set. Also, the attacks "Perl", "PHF", and "Spy" each had only one record in the test set. Thus, for all of these attacks, the calculated "Class Acc. (%)" are not reliable indicators of the misuse classifier's ability to discern those attacks. However, the "Normal" records still showed a high rate of success.

TABLE I. Classification Time

IDS Type	**Running Time (s)**	
	Building the model	***Testing the model***
Misuse	386.18	5.50
Anomaly	368.32	3.75

TABLE II. OVERALL ACCURACY

IDS Type	Accuracy (%)
Misuse	99.9773
Anomaly	99.9891

TABLE III. ANOMALY RESULTS

Actual Class	Determined Class		Class Acc. (%)
	Normal	Anomaly	
Normal	173174	6	99.9965
Anomaly	21	73810	99.9716
Determination Acc. (%) †	99.9879	99.9919	

†: Horizontal

TABLE IV. MISUSE RESULTS

Actual Class	Determined Class																							Class Acc. (%)
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
A	317	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100.0000
B	0	7	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	87.5000
C	0	0	1	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	20.0000
D	0	0	0	11	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	91.6667
E	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	N/A *
F	0	0	0	0	0	1071	0	0	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	99.3506
G	0	0	0	0	0	0	6	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	75.0000
H	0	0	0	0	0	0	0	1	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	33.3333
I	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	N/A *
J	0	0	0	0	0	0	0	0	0	67989	0	0	0	0	0	0	0	0	0	0	0	0	0	100.0000
K	0	0	0	0	0	9	0	0	0	0	482	0	0	0	0	0	0	0	0	0	0	0	0	98.1670
L	0	0	0	0	0	0	0	0	1	0	1	173173	0	0	0	0	1	0	0	0	0	4	0	99.9960
M	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	100.0000
N	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	100.0000
O	0	0	0	0	0	0	0	0	0	0	0	0	0	0	67	0	0	0	0	0	0	0	0	100.0000
P	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	905	0	0	0	0	0	0	0	99.8896
Q	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	1	0	0	0	0	0	0.0000
R	0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	1	0	1480	0	0	0	0	0	99.3289
S	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	900	0	1	0	0	99.8890
T	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0.0000
U	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	281	0	0	100.0000
V	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	258	0	98.4733
W	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	4	66.6667
Determination Acc. (%) †	100.0000	100.0000	100.0000	100.0000	N/A **	99.1667	100.0000	100.0000	0.0000	99.9971	98.5685	99.9838	100.0000	100.0000	100.0000	99.8896	0.0000	99.9325	100.0000	N/A **	99.6454	98.4733	100.0000	

A: Back B: BufferOverflow C: FTPWrite D: GuessPassword E: Imap F: IPSweep G: Land
H: LoadModule I: MultiHop J: Neptune K: NMap L: Normal M: Perl N:PHF
O: Pod P: PortSweep Q: RootKit R: Satan S: Smurf T: Spy U: TearDrop
V: WarezClient W: WarezMaster *: None of this type were in the test set ⁑: No determined instances to compare †: Horizontal