International Journal of Cyber-Security and Digital Forensics (IJCSDF) 5(2): 106-114
The Society of Digital Information and Wireless Communications, 2016 (ISSN: 2305-0012)

Enhancing Performance of Intrusion Detection System Against KDD99 Dataset Using Evidence Theory

Vrushank Shah[1] and A. K. Aggarwal[2]
[1]Assistant Professor, Indus University, Ahmedabad, India
[2]Vice Chancellor, Gujarat Technological University, Ahmedabad, India
[1]Vrushank26@yahoo.in , [2]vc@gtu.ac.in

ABSTRACT

The rapid growth of internet and its related technology requires an efficient method to detect intrusion or attack in the network. Intrusion detection system is a system that detect an attack and raise an alert for any abnormal situation. However, the existing intrusion detectors produces a large number of false alerts and it became a difficult situation for a network administrator to cope with large number of false alerts. To overcome such situation and to increase the detection rate of intrusion detection system we propose a method to fuse alerts from multiple intrusion detection system using evidence theory. Evidence theory is a mathematical theory of evidence which is used to fuse evidence from multiple sources of evidence and outputs a global decision. The work in these paper discusses the limitations and issues with evidence theory and proposes a modified framework for fusion of multiple intrusion detection system.

KEYWORDS

Intrusion Detection, KDD, Evidence Theory, DS rule, reliability

1 INTRODUCTION

In today's digital world, there is a big influence of internet on our daily life. Now businesses all over the world has goes online and internet has become a tool for easy access of information. However, along with ethical use of internet, some people try to use internet for unethical activities. This becomes very risky as they can access highly confidential data and information by intrusion in these computer network systems. An intrusion is defined as any sets of action in order to violate the security policy of a computer network system. An intrusion can be performed in order to gather information about one or more machine or services used by the machine. It can be performed in order to interrupt or degrade the services provided by machine on the network. The intrusion can be done by a legitimate user which may try to break security by gaining root access or it can be performed completely by illegitimate user. With rapid growth in modern technology, intruder uses mechanisms to intrude into network which are highly difficult to detect with the use of traditional firewalls, security policies or any other mechanism [1]. Intrusion detection system is a tool that sniffs the network traffic and raises an alert for any abnormal situation which occur despite of other security policies. There is tremendous research going on in order to improve efficiency of intrusion detection system. The major work in the field of intrusion detection system can be found in [2, 3, 4, 5].

The performance of intrusion detection system in detecting the true intrusion or attack is highly questionable because most of the intrusion detection system produce large number of false positives. These will create an additional adhoc on the system administrator for evaluating each of these alerts. Along with these, the performance evaluation process of an intrusion detection is also a challenging task. Usually, the intrusion detection performance testing can be done in actual environment where it has to be deployed which is called as online evaluation. However, offline evaluation of intrusion detection system is preferable as the researchers often do not have any access to the computer network system for testing the intrusion detection system. The offline evaluation of IDS is done using the standard test dataset which is very similar to the real environment situation. One such dataset called KDD99 is available online at http://www.kdd.ics.uci.edu and was used by many researchers to test their intrusion detection

system. The present work proposes an approach to improve performance of intrusion detection system using evidence theory [8] and the proposed approach is being tested against KDD99 dataset.

Intrusion detection system usually falls into two major types namely, signature or misuse intrusion detection system and anomaly intrusion detection system. A signature based intrusion detection system sniffs the incoming packet and compares them against a database of signatures or attributes from known malicious intrusions. These signature based intrusion detection systems are capable of detecting only known intrusions and fail to detect zero-day intrusion in computer network system [6].

An anomaly based intrusion detection system sniffs the incoming packet and compares them against an established baseline. The baseline identifies the normal behavior of the network and any abnormal situation created by an intrusion is detected. Nong Ye in [7] presents the alert fusion process and shows that when anomaly detection techniques and signature recognition techniques are applied simultaneously to the same observed activities of computer and network systems, anomaly detection techniques and signature recognition techniques complement one another for achieving a high detection rate and a low false alarm rate.

The proposed approach shows the alert fusion of multiple intrusion detection system in order to combines advantages of anomaly and signature based type with the help of evidence theory as proposed by Shafer in [8].

2 BACKGROUND

Evidence theory is a mathematical theory to combine the evidence from multiple sources of information to calculate the probability of an event. The Dempster-Shafer theory proposed by Arthur dempster in 1968 and modified by Glenn Shafer in 1976 [8] is the first mathematical theory propose to combine uncertain information of sources to make an inference. The fusion rule proposed under dempster-shafer framework is called as Dempster-Shafer's rule. Dempster-shafer's rule has been a topic of debate for researchers working in the field of information fusion.

The fusion theory is used to combine masses from n evidence sources and outputs a fused decision. For number of evidence sources $n \geq 2$ let $\Theta = \{\theta_1, \theta_2, \theta_3, \ldots, \theta_n\}$ be the frame of discernment for the fusion problem under consideration having n exclusive and exhaustive hypothesis θ_i. The sets of all subsets of Θ is called as power-set of Θ and is denoted by 2^{Θ}. In shafer's framework by shafer (1976), the basic belief assignment (bba) $m(.): 2^{\Theta} \rightarrow [0,1]$ is assigned to all elements within the powerset of Θ. The mass assignment will satisfy the property.

$$m(\emptyset) = 0 \; and \sum_{A \in 2^{\Theta}} m(A) = 1 \qquad (1)$$

Let, $m_1(B)$ and $m_2(C)$ are two independent masses from two sources of evidence. Then the combined mass m(A) is obtained by combining $m_1(B)$and $m_2(C)$ through the rule

$$m(A) = \frac{\sum_{\substack{B,C \in 2^{\Theta} \\ B \cap C = A}} m_1(B) m_2(C)}{1 - \sum_{\substack{B,C \in 2^{\Theta} \\ B \cap C = \emptyset}} m_1(B) m_2(C)} \qquad (2)$$
$$m(\emptyset) = 0$$

The above rule is defined for fusing two independent masses from sources of evidence. However, the same can be extended for n independent and equally reliable sources.

3 CLASSICAL ALERT FUSION

Intrusion detection system is a classifier which classifies an input packet as either normal or abnormal. Intrusion Detectors sniffs the network and collect evidences about the presence of an intrusion/attack. The evidence provided are usually incomplete, uncertain, contradictory or conflicting and can be complementary. The failure of single IDS in a network usually occur due to the fact that IDS are very precise in detecting a particular class of attack and is completely imprecise or partially imprecise for other classes. Thus the usage of single IDS as a classifier doesn't ensure a correct detection of abnormality in all cases. For events involving multiple classes of attack the fusion of multiple intrusion detection system is ideal solution. The use of multiple IDS or multiple classifier is demonstrated by Chen and Aickelin [3] and Yu and Frincke [9] and is identified as the method to improve the accuracy of IDS for detection of abnormalities. Thus fusion of

multiple IDS can be defined as a process that merge the evidence provided by IDS and classifies it as either normal or abnormal situation.

The classical method of fusing evidences from multiple intrusion detection systems is as shown in figure-1

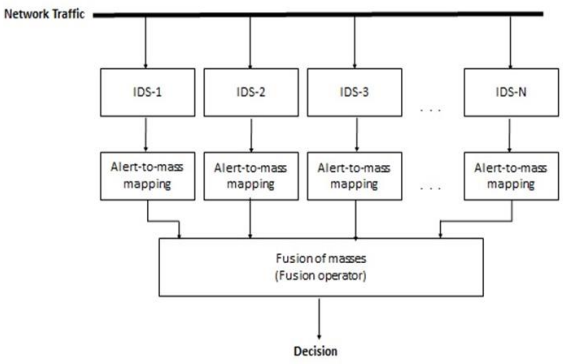

Figure-1 Flowchart of the classical method of fusing evidences from multiple intrusion detection systems

The classical approach assume all the IDS to be equally reliable and assign same weightage to each of the evidences. However, in real scenario it is not true because some IDS are dominant for detecting certain class of attack and also its evidence can be more reliable compared to other IDS involved in fusion process. Reliability of Intrusion Detection system is defined as the ability of system to correctly classify the input packet. Reliability parameter is utilized as a discounting factor to discount the evidence of conflicting or complementary and unreliable IDS and then discounted evidences will be fused to make a decision about the presence of attack. We propose a novel fusion operator that fuses the alerts from multiple IDS and also incorporates reliability value related to each IDS.

As shown in figure-1 the classical method for combining alerts from N different Intrusion Detection system, Each IDS sniffs the incoming network traffic and raise positive and negative alerts for the presence of an attack. The Alerts generated by IDS is converted to a mass value and all such masses are fused by fusion operator. If we denote the hypothesis that attack is present by A and attack not present by –A then,

$$m(A) = \frac{P}{P+N+C} \quad (3)$$

$$m(-A) = \frac{N}{P+N+C} \quad (4)$$

$$m(-A\ or\ A) = \frac{C}{P+N+C} \quad (5)$$

Here, P- positive evidence in favour of hypothesis A, N-Negative evidence opposing the hypothesis A or favoring hypothesis –A and C is constant which is equal to 2 for binary frame of hypothesis. m(A) is the mass value for hypothesis A. m(-A or A) is mass value for hypothesis A or –A and can be called m(u) i.e, mass value for uncertainty between A and –A.

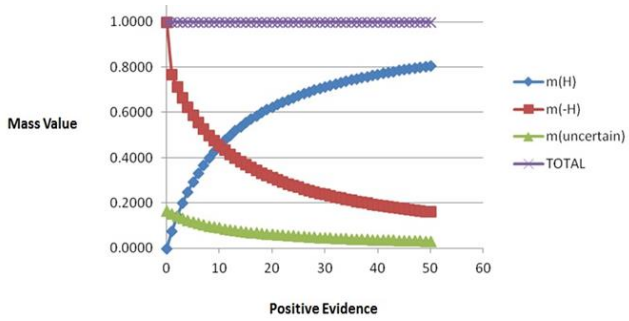

Figure-2 Positive evidence versus belief mass value favoring and opposing an hypothesis

4 REQUIREMENTS AND LIMITATIONS OF ALERT FUSION RULE

Ciza Thomas [10] suggests that the timely detection of intrusion in multiple IDS framework requires an efficient fusion rule that effectively combines evidence from multiple IDS and outputs a decision that accurately matches with existing ground truth. Following are the basic requirements for fusion rule as mapped out by authors:

i) Fusion rule should incorporate the reliability of intrusion detection system for the evidence it provide about the presence of intrusion.

ii) The fusion should be able to compromise between the reliable IDS and unreliable IDS.

iii) If the all the IDS involved in fusion are unreliable then fusion rule should discard the available IDS and then new sets of IDS has to be found for concerned fusion problem.

In the field of fusion theory everything depends upon the type of application or the problem [4]. Since in present work we are concerned with combining the alerts of various intrusion detection systems, it is necessary that the alerts generated is trustworthy. The existing fusion rules discussed in [11, 12] has following limitations.

i) None of the existing rule incorporates the reliability of source whose evidence are to be fused. Thus, there is no real time criteria which assign a numerical value of reliability to the evidence given by the source.

ii) The existing fusion rule considered all the sources of evidence to be equally reliable. However, in fusion framework there might be some unreliable sources which misleads to the fusion rule to give wrong decision.

iii) One major drawback related to the fusion rule as suggested by Goodman [13] is that in an environment consisting of many hypotheses and many sources, it is difficult to decide whether to accept or reject the result of such fusion rule. If sources of evidences are highly conflicting, the DS rule completely fails. If analyst blindly believes on the result then the decision can be misleading or complementary.

Thus, we need a framework which can evaluate the numerical value of reliability of intrusion detection systems and discount the evidences based on their reliability beforehand. Also, there must be robust way as to handle conflict between sources and uncertainty assigned by sources to hypotheses.

5 PROPOSED ALERT FUSION

To overcome the limitations and to match the requirements for fusion rule. These section discusses a novel method of fusing the evidences provided by source (Alerts generated by Intrusion Detection System). The proposed rule is based on Shafer's framework. Here, $m_1(B)$ and $m_2(C)$ are

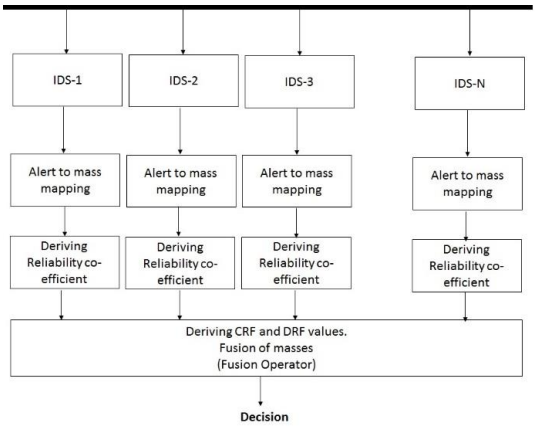

Figure-3 Flowchart of the proposed method of fusing evidences from multiple intrusion detection systems

two independent masses from two sources of evidence. Then the combined mass m(A) is obtained by combining $m_1(B)$and $m_2(C)$ through the rule given by equation (6)

Here Rn is the reliability value of nth source of evidence. CRF(A) is conjunctive reliability value and DRF(A) is disjunctive reliability value. CRF and DRF value acts as a weighting factor to compromise between conjunctive mass and disjunctive mass. These values can be derived using following formulas given in equation (7) and (8).

$$m(A) = \left[CRF(A) \sum_{\substack{B,C \in 2^{\Theta} \\ B \cap C = A}} m_1(B) m_2(C)) + DRF(A) \sum_{\substack{B,C \in 2^{\Theta} \\ B \cup C = A}} m_1(B) m_2(C) \right] \quad (6)$$

$$CRF(A) = \prod_n R_n \quad (7)$$

$$DRF(A) = [1 - [\prod_n R_n]][1 - [\prod_n (1 - R_n)]] \quad (8)$$

One of the major problems of incorporating reliability of IDS into the fusion is problem of obtaining reliability coefficients. Reliability coefficients basically show a numerical value of trust in the mass value provided the Intrusion Detection system. The problem of finding reliability can be related to the problem of conflict between various Intrusion detection systems. The mere existence of conflict between the mass provided by Intrusion detection systems indicates the presence of an unreliable IDS which may cause the fusion result to be complementary from reality.

Another Approach of finding reliability is to relate reliability with the true alert rate of IDS. In these approach it is assumed that the IDS having highest true alert rate and lowest false alert rate will be assigned highest reliability and thereby, given highest weightage in fusion process. While, all other IDS is assigned relative reliability value based on their true alert rate and false alert rate. The approach of assigning reliability based on true alert rate requires the ground truth knowledge. While, the approach of assigning reliability based on conflict between the IDS can work without knowledge of ground truth. In these work, we will use both the approach and compare result of proposed rule with existing rules.

6 KDD99 DATASET

KDD is the abbreviation of knowledge discovery in databases. KDD refers to overall process of recovering knowledge from data. Specifically KDD99 is designed for evaluation of intrusion in computer networks [13]. It is like a benchmark on which many researchers has tested their methodologies.

Table-1 Types of Attack categories in KDD'99 dataset [13]

Attack type	Sub Attack types
DOS	Smurf, teardrop, pod, back, land, apache2, udpstrom, mailbomb, processtable, Neptune
Probe	Ipsweep, portsweep, nmap, satan, saint, mscan
U2R	Buffer_overflow, rootkit, perl, loadmodule
R2L	Imap, ftp_write, guess_passwd, multihop, phf, spy, warezclient, warezmaster

The dataset is available in tcpdump format. The original tcpdump files were preprocessed for utilization of intrusion detection benchmark. KDD99 dataset consists of 4,900,000 single connection vectors each of which contains 41 features and is labeled as either normal or an attack. The attack falls in one of the types and subtypes shown in table-1. The list of 41 features of dataset is shown in appendix [13].

6 EXPERIMENTAL RESULTS

For Alert fusion of multiple Intrusion Detection Systems, Four heterogeneous intrusion detection systems namely, Snort, Suricata, PHAD and NETAD has been selected. The reason behind such selection is that snort and suricata are signature based intrusion detectors while PHAD and NETAD are anomaly detectors. Thus, both types are complementary to one another which enhances the performance of fused IDS. The simulation environment consists three 3rd Generation Intel®Core™i5processor (1.6GHz), Operating system installed is Linux Ubuntu with 4GB RAM. One machine deployed with Signature based IDS such as snort and suricata. Another Machine deployed with Anomaly detectors such as PHAD and NETAD. Third machine acts as an attacker machine having KDD99. The KDD99 was preprocessed and then total 3456 packets containing attack and non-attacks packets in various types was loaded on the network and is replayed using TCPREPLAY tool.

In present experiment we strictly focus on detection of smurf attacks. Thus, for these experiment our frame of discernment is Θ = {smurf,-smurf, θ} The total smurf attack present in dataset is 1944. Table-1 and Table-2 shows the statistics obtained when KDD99 is tested against Snort, Suricata, PHAD and NETAD. Table-2 and Table-3 also shows the result obtained by fusion of alerts from all the four IDS with DS operator and proposed rule. Here, we have derived the reliability by finding the amount of conflict between alerts given by four Intrusion Detection Systems. The IDS having minimum conflict with other IDS will be assigned highest reliability and all other IDS will be assigned relative reliability value.

In above table, TP=True positive, FP=False positive, TN=True Negative, FN=False Negative, TPR=True Positive Rate, FPR=False positive rate, PPV=Positive Prediction value and NPV=Negative prediction value. True positives are the number of events in which intrusion detector detects the attack and the computer network is under attack. True negatives are the number of events in which intrusion detector doesn't detect the attack and the computer network is

also not under attack. False negatives are the number of events in which intrusion detector doesn't detects the attack and the computer network is under attack. False positives are the number of events in which intrusion detector detects an attack and the computer network is not under attack. True positive rate is the ratio of total true positives and sum of true positives with false negatives. False positive rate is the ratio of total false positives and sum of false positives with true negatives. Positive prediction value is the ratio of total true positives and sum of true positives with false positives. Negative prediction value is the ratio of total true negative and sum of true negatives with false negatives. Accuracy is the ratio of sum of true positives and true negatives with the sum of true positives, false negatives, true negative and false positives.

Table-4 and Table-5 shows the statistics obtained when KDD99 is tested against Snort, Suricata, PHAD and NETAD. Table-4 and Table-5 also shows the result of obtained by fusion of alerts from all the four IDS with DS operator and proposed rule. Here, we have derived the reliability using second approach as discussed in section 3.2. In these approach reliability is related to true positive rate. An IDS giving highest true alerts will be assigned highest reliability.

8 CONCLUSION

In this paper, a reliable alert fusion approach is proposed which is designed to make compromise between conjunctive logic and disjunctive logic. The simulation result shows the performance of proposed approach with an improvement in false positive rate. These has been shown for KDD99. The research in the paper defines two new parameters namely conjunctive reliability parameter (CRF) and disjunctive reliability parameter (DRF), the values of which are derived using two approaches of reliability.

9 REFERENCES

1. Kendall, K., 1999. A database of computer attacks for the evaluation of intrusion detection systems. Massachusetts Inst Of Tech Cambridge Dept Of Electrical Engineering And Computer Science.
2. Siaterlis, C. and Maglaris, B., 2004, March. Towards multisensor data fusion for DoS detection. In Proceedings of the 2004 ACM symposium on Applied computing (pp. 439-446). ACM.
3. Chen, Q. and Aickelin, U., 2006. Anomaly Detection Using the Dempster-Shafer Method. In DMIN (pp. 232-240).
4. Katar, C., 2006. Combining multiple techniques for intrusion detection. Int J Comput Sci Network Security, 6(2B), pp.208-218.
5. Axelsson, S., 2000. Intrusion detection systems: A survey and taxonomy(Vol. 99). Chalmers University of Technology, Goteborg, Sweden: Technical report.
6. Kenkre, P.S., Pai, A. and Colaco, L., 2015. Real time intrusion detection and prevention system. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014(pp. 405-411). Springer International Publishing.
7. Ye, N., Li, X., Chen, Q., Emran, S.M. and Xu, M., 2001. Probabilistic techniques for intrusion detection based on computer audit data. Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on,31(4), pp.266-274.
8. Shafer, G., 1976. A mathematical theory of evidence (Vol. 1, pp. xiii+-297). Princeton: Princeton university press.
9. Yu, D. and Frincke, D., 2005, March. Alert confidence fusion in intrusion detection systems with extended Dempster-Shafer theory. In Proceedings of the 43rd annual Southeast regional conference-Volume 2 (pp. 142-147). ACM
10. Thomas, C. and Balakrishnan, N., 2009. Improvement in intrusion detection with advances in sensor fusion. Information Forensics and Security, IEEE Transactions on, 4(3), pp.542-551.
11. Smarandache, F. and Dezert, J. eds., 2006. Advances and Applications of DSmT for Information Fusion (Collected works), second volume: Collected Works (Vol. 2). Infinite Study.
12. Goodman, I.R., Mahler, R.P. and Nguyen, H.T., 2013. Mathematics of data fusion (Vol. 37). Springer Science & Business Media.
13. KDD data set, 1999; http://kdd.ics.uci.edu/databases/-kddcup99/kddcup99.html

Table-2 Comparison of Individual IDS with Fusion with DS and fusion with proposed rule in terms of TP, TN, FN and FP

	Snort	Suricata	PHAD	NETAD	Fusion with DS Operator	Fusion with proposed rule
TP	997	967	1015	960	1008	1033
TN	742	741	730	758	723	1501
FP	770	771	782	754	789	11
FN	947	977	929	984	936	911

Table-3 Comparison of Individual IDS with Fusion with DS and fusion with proposed rule in terms of PPV, NPV, TPR, FPR and ACCURACY

	Snort	Suricata	PHAD	NETAD	Fusion with DS Operator	Fusion with proposed rule
TPR	0.5129	0.4974	0.5221	0.4938	0.5185	0.5314
FPR	0.5093	0.5099	0.5172	0.4987	0.5218	0.0073
PPV	0.5642	0.5564	0.5648	0.5601	0.5609	0.9895
NPV	0.4393	0.4313	0.4400	0.4351	0.4358	0.6223
ACCURACY	0.5032	0.4942	0.5049	0.4971	0.5009	0.7332

Table-4 Comparison of Individual IDS with Fusion with DS and fusion with proposed rule in terms of TP, TN, FN and FP

	Snort	Suricata	PHAD	NETAD	Fusion with DS Operator	Fusion with proposed rule
TP	916	1015	982	910	969	1015
TN	788	763	769	762	765	1490
FP	724	749	743	750	747	22
FN	1028	928	962	1034	975	929

Table-5 Comparison of Individual IDS with Fusion with DS and fusion with proposed rule in terms of PPV, NPV, TPR, FPR and ACCURACY

	Snort	Suricata	PHAD	NETAD	Fusion with DS Operator	Fusion with proposed rule
TPR	0.4712	0.5221	0.5051	0.4681	0.4985	0.5216
FPR	0.4788	0.4954	0.4914	0.4960	0.4940	0.0146
PPV	0.5545	0.5754	0.5693	0.5482	0.5647	0.9788
NPV	0.4339	0.4509	0.4443	0.4243	0.4397	0.6160
ACCURACY	0.4931	0.5145	0.5067	0.4838	0.5017	0.7248

Appendix: KDD'99 Features List [13]

Feature number	Feature Name	Description
1	Count	No. of connections to the same host as the current connection in the last two seconds
2	destination bytes	Bytes sent from destination to source
3	diff srv rate	percentage of connections to different services
4	dst host count	count of connections having the same destination hosts
5	dst host diff srv rate	percentage of different services on the current host
6	dst host rerror rate	percentage of connections to the current host that have an RST error
7	dst host same src port rate	percentage of connections to the current host having the same src port
8	dst host same srv rate	percentage of connections having the same destination host and using the same service
9	dst host serror rate	percentage of connections to the current host that have an S0 error
10	dst host srv count	count of connections having the same destination host and using the same service
11	dst host srv diff host rate	percentage of connections to the sameservice coming from different hosts
12	dst host srv rerror rate	percentage of connections to the current host and specified service that have an RST error
13	dst host srv serror rate	percentage of connections to the current host and specified service that have an S0 error
14	Duration	Duration of the active connection
15	Flag	Status flag of the Connection
16	Hot	No. of "hot" indicators
17	is guest login	1 if the login is a "guest" login; Otherwise 0
18	is host login	1 If the login belongs to the "host"; otherwise 0
19	Land	1 if connection is from/to the samehost/port; Otherwise 0

20	logged in	1 if successfully logged in; otherwise 0
21	num access files	No. of operations on access control files
22	num compromised	No. of compromised conditions
23	num failed logins	No. of failed logins
24	num file creations	No. of file creation operations
25	num outbound cmds	No. of outbound commands in an ftp session
26	num root	No. of "root" accesses
27	num shells	No. of shell prompts
28	protocol type	Connection protocol (e.g. tcp, udp).
29	rerror rate	percentage of connections that have “REJ" Errors
30	root shell	1 if root shell is obtained; otherwise 0
31	same srv rate	percentage of connections to the same service
32	serror rate	percentage of connections that have “SYN" Errors
33	Service	Destination service (e.g. telnet, ftp)
34	src bytes	Bytes sent from source to destination
35	srv count	No. of connections to the same service as the current connection in the last two seconds
36	srv diff host rate	percentage of connections to different hosts
37	srv rerror rate	percentage of connections that have “REJ" errors
38	srv serror rate	percentage of connections that have “SYN" Errors
39	su attempted	1 if "su root" command attempted; otherwise 0
40	Urgent	No. of urgent packets
41	Wrong fragment	No. of wrong fragments