International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.8, pp : 1082-1084 1 Aug 2014

Intrusion Detection System (IDS) Using Layered Based Approach For Finding Attack

Suman Bharti, Dr. Savita shiwani, Dinesh Goyal, Vinit Agrawal
Jaipur, India India, Sumanbharti.sgvu@gmail.com

Abstract- ***Intrusion detection system(IDS) is must to detect malicious activity in a network. In this paper we are concentrating on accuracy and efficiency in network to detect whether the packet as intruder element . We are using layered based approach , with this approach more time is saved . There are four layers in this system probe , DoS, R2L, and U2R, a packet first checked for probe attack first if there is attack then the packet is dropped. If there is no attack it will pass to DoS layer. Similar approach is taken for other three layers. There are 41 features to detect whether the packet affected or not. It is not necessary to check all 41 features in all the layers for this CRF mechanism is used with this approach we can detect the attack efficiently and accurately.***

Keywords- intrusion detection, layered based, CRF, kdd99.

I. Introduction-

Intrusion detection system was introduce in SANS institute in 1980s[6] . IDS is the tools/software that monitors the network and which is used for the detecting attack on the network when unauthorized user wants to access to network in that case we can used IDS for the more security[1]. it work as firewall it provides more security than firewall, virus etc. In this paper we are concentrating on the accuracy and efficiency in network to detect whether the packet as intruder element. Intrusion detection system is classified in the two categories .

First one is Host based and second one is network based system.

Host Base IDS- Host base IDS work on the individual host or device on the network it handles the intruders only on incoming and outgoing on the device and then it report to the administration and its alert.

Network Base IDS- Network base IDS works on hole system. NIDS device is keep at one space on the network than it protect to hole system anywhere when attack came in network in anywhere in the network.Intrusion detection system is further classified into categories. First one is signature based system and second one anomaly based system.

Signature base system- Signature based system will check packet firstly and it compare with the database signature. Other method is used for the detection of attack on the network hybrid system because it contains both approach signature base and anomaly base system.

In section2 proposed work and methodology which is using for intrusion detection such as conditional random field(CRF)[2]. and layered based approach . In section3 shows the result and conclusion of proposed system and then conclusion and acknowledgment and. Section4 references.

II. Proposed Work

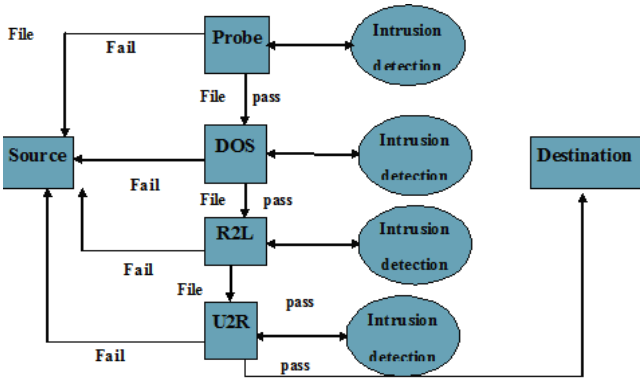
For intrusion detection using layered based approach in this approach we are using four layers which will show below it compare with the kdd99 DATA SET as below table1 this is downloaded we are only use it and it will compare the packet[3][15]. And there is 41 features to check whether the packet the packet affected or not using conditional random field(CRF) but there is no compulsory that all 41 features to can check into the all layers efficiently or accurately.

TABLE1

	Training set	Test set
Normal	97,277	60,593
Probe	4,107	4,166
DoS	391,458	229,853
R2L	1,126	16,349
U2R	52	68
Total	494,020	311,029

Layerd Based Approach

We are using four layers probe layer, Dos layer, U2R layer and R2L layer. Diagram mention below this is the working of proposed system in this architecture shows this architecture check firstly probe layer packet check first and it will check for probe attack if there is attack and then it will dropped there and if there is no attack it will pass to the next layer DoS layer. and similarly further another three layer works same process. For example Airport security Model, In this model number of security available for checking to all members which suffer in plane and firstly checking here such as visa, and identity proof in sequence manner similarly LIDS works in same manner in sequence and it protect to hole system over network.



Conditional Random Field(CRF)- Conditional random field is one of the method which is used in this proposed system for reduce the computation and also we are using LIDS approach for

reduce overall time for detect malicious activity/attack in network and protect to hole system. Here both approach are combined and compare with the kdd99 data set because we are using 41 features each layer select specific features such as probe layer select only 5 features, DoS layer select 9 features, R2L select 14 features and U2R layer select 8 features .

Features selection- In our system , we are choose 4 layers and here select feature each and every layer individually and categorised it off different type of attack base on layered base approach and type of attack have been trained and detect it.

Probe layer- Probe layer is taking the information about the destination that number of file creation and accessed it. In probe layer select 5 feature only.

DoS layer- DoS layer is mainly it will force to the target to stop the services and it provides flooding means eliminate the request. In DoS layer select 9 feature only.

R2L Layer- R2L layer is one of the layer in which both type of feature can be select like network level and host level feature. In the network level feature such as duration of connection and service requested and host level feature such as number of failed logging. In R2L layer select 14 feature only.

U2R Layer- user to request layer is one of the layer in which select the feature different type such as number of file creation and number of shell prompts when we ignored features such as protocol and source byte. In U2R layer select 8 feature only.

Probe layer feature selection

Feature number	Feature name
1	Duration
2	Protocol-type
3	Service
4	Flag
5	Src-byte

DoS layer features selection

1	Duration
2	Protocol-type
3	Flag
5	Src-byte
23	Count
34	Dst_host_same_srv_rate
38	Dst_host_serror_rate
39	Dst_host_serv_serror_rate
40	Dst_host_rerror_rate

R2L layer features selection

Features number	Features number
1	Duration
2	Protocol_type
3	Service
4	Flag
5	Src_byte
10	Host
11	Num_failed_logins
12	Logged_in
13	Num_compermised
17	Num_files_creations
18	Num_shells
19	Num_access_files
22	Is_guest_login

U2R layer features selection

Features number	Features name
10	Host
13	Num_compermised
14	Root_shell
16	Num_root
17	Num_files_creations
18	Num_shells
19	Num_access_files
21	Is_host_login

algorithm

Training

Step1: suppose n is the number of layers.

Step2: perform feature separately to each layer of entire system.

Step3: Train it for separately each layer with CRF for each layer from step2

Step4: and it plug into the trained model sequentially connection labeled feature as normal and it pass to the next layer.

Testing

Step5: for each test and perform to next step through step9.

Step6: test it and labeled it either attack or normal.

Step7: if there is attack in labeled then block it and identify it attack represented by layer name and detect and go to the step5

Else it will pass to the next layer.

Step8: if the current layer is not last layer of system then it will test while its not last layer system.

Else go to the step9

Step9: test while labeled is normal or as attack. If the instance labeled is as attack it will block and identify the attack name.

III. Result and Tables

We are using kdd99 data set in this database compare with the more than method such as naive Bayes, k-means clustering, etc. Here we are using conditional random field with layered based approach this approach is better than the another method because its attack detection accuracy and efficiency is better to another method selecting 41 features and features is categories in different layer which is show above. Here result is compare the result with layered and non-layered approach there is mention here that accuracy in percentage and efficiency as shown in below table and also there is output which is given kdd99 data set it gives protocol etc.

			Attack detection in percentage				Time (sec)
			probe	DoS	R2L	U2R	
layered	layered	Feature selection	98.62	97.40	29.62	86.33	17
		All features	88.06	97.05	15.10	55.03	56
Non-Layerd	Non-layered	Features selection	92.21	96.88	16.01	60.00	29
		All features	87.94	96.12	17.58	48.24	57

In this table shows here CRF have very high attack detection method with layered approach.

For probe layer it detect 98.6 percent with improvement 5.8 percent , for DoS layer 97.40 percent with improvement 5.8 percent , for R2L layer improvement 34.5 percent and last layer U2R layer improvement attack detection with 34.8 percent attack.

Conclusion

In this paper , we have found two problem first one is accuracy and second one is efficiency for build system using intrusion detection system. Our experimental result shows in section3 CRF is very highly attack detection with layered based approach for improvement attack detection rate and decreasing FAR and further feature selection and implementing the layered approach and reduce the required and test the model and percentage is show above.

Acknowledgment

The authors sincerely thank the anonymous reviewers whose comments have greatly helped clarify and improve this paper.

References

i. Autonomous Agents for Intrusion Detection, http://www.cerias. purdue.edu/research/aafid/, 2010.

ii. CRF++: Yet Another CRF Toolkit, http://crfpp.sourceforge.net/, 2010.

iii. KDD Cup 1999 Intrusion Detection Data, http://kdd.ics.uci.edu/ databases/kddcup99/kddcup99.html, 2010.

iv. Overview of Attack Trends, http://www.cert.org/archive/pdf/ attack_trends.pdf, 2002.

v. Probabilistic Agent Based Intrusion Detection, http://www.cse.sc. edu/research/isl/agentIDS.shtml, 2010.

vi. SANS Institute—Intrusion Detection FAQ, http://www.sans.org/ resources/idfaq/, 2010.

vii. T. Abraham, IDDM: Intrusion Detection Using Data Mining Techniques, http://www.dsto.defence./gov.au/publications/ 2345/DSTO-GD-0286.pdf, 2008

viii. . R. Agrawal, T. Imielinski, and A. Swami, "Mining Association Rules between Sets of Items in Large Databases," Proc. ACM SIGMOD, vol. 22, no. 2, pp. 207-216, 1993.

ix. N.B. Amor, S. Benferhat, and Z. Elouedi, "Naive Bayes vs. Decision Trees in Intrusion Detection Systems," Proc. ACM Symp. Applied Computing (SAC '04), pp. 420-424, 2004.

x. J.P. Anderson, Computer Security Threat Monitoring and Surveillance, http://csrc.nist.gov/publications/history/ande80.pdf, 2010.

xi. . Benhamou, "Distributed Intrusion Detection Framework Based on Mobile Agents," Proc. Int'l Conf. Dependability of Computer Systems (DepCoS-RELCOMEX '06), pp. 248-255, 2006.

xii. Y. Bouzida and S. Gombault, "Eigenconnections to Intrusion Detection," Security and Protection in Information Processing Systems, pp. 241-258, 2004.

xiii. H. Debar, M. Becke, and D. Siboni, "A Neural Network Component for an Intrusion Detection System," Proc. IEEE Symp. Research in Security and Privacy (RSP '92), pp. 240-250, 1992.

xiv. T.G. Dietterich, "Machine Learning for Sequential Data: A Review," Proc. Joint IAPR Int'l Workshop Structural, Syntactic, and Statistical Pattern Recognition (SSPR/SPR '02), LNCS 2396, pp. 15-30, 2002.

xv. K.K. Gupta, B. Nath, and R. Kotagiri, "Conditional Random Fields for Intrusion Detection," Proc. 21st Int'l Conf. Advanced Information Networking and Applications Workshops (AINAW '07), pp. 203-208, 2007.

xvi. *K.K. Gupta, B. Nath, R. Kotagiri, and A. Kazi, "Attacking Confidentiality: An Agent Based Approach," Proc. IEEE Int'l Conf. Intelligence and Security Informatics (ISI '06), vol. 3975, pp. 285-296, 2006.*

xvii. *M. Sabhnani and G. Serpen, "Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context," Proc. Int'l Conf. Machine Learning, Models, Technologies and Applications (MLMTA '03), pp. 209-215, 2003.*