IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

An Overview Of Intrusion Detection System Using Various Classification Concepts

K Shukla[1*], R K Gupta[2], V. Namdeo[3]

[1] Department of Computer Science, SRK University, Bhopal, India
[2] Department of Computer Science, SRK University, Bhopal, India
[3] Department of Computer Science, SRK University, Bhopal, India

[*]*Corresponding Author: csresearch2018@gmail.com, Tel.:9131537884*

Available online at: www.ijcseonline.org

Accepted: 16/Nov/2018, Published: 30/Nov/2018

***Abstract*—** As technological interconnection and digital communication schemes wide spreading, data accessing required to be kept in sharing environment and hence it will surely lead to compromise the data in many aspects. So to keep data secure and protected there are variety of techniques and tools also developed and Intrusion detection system (IDS) is one of them. IDS system conceptualized with identifying the intrusions in place of stopping the attacks. There are various techniques discussed here in context of signature and behavior based IDS. These IDS tools use different identification techniques to classify and identify the attacks and type of attacks. This paper includes different types IDS which has capability inclusion of identifying attacks like probe, DoS, R2L etc. It is also covering categorized descriptions of host based as well as network based hybrid intrusion detection systems.

***Keywords*—**Attacks, Classification, Communication, Detection, DoS, Intrusion, R2L, Signature etc.

I. INTRODUCTION

With the huge growth of computer networks usage and internet accessibility, more organizations are becoming susceptible to a wide variety of attacks and threats. Information plethora being generated in an organization tends to the evolution of cloud computing technologies for efficient management and accessibility of voluminous data. With increased utilization of cloud computing by organizations working in different domains, several new security threats have been encountered. In recent time, ensuring security to the cloud platforms is one of the key challenges. In case of highly distributed systems, the threat of malicious content or behaviour form network side itself is considered to be the most challenging one. In particular, we have proposed a hybrid intrusion detection algorithm for host-based intrusion detection. Based on proposed algorithm, a hybrid intrusion system has been developed namely, HyINT, which uses both signature and anomaly-based detection methodologies. Also, different parameters have been discussed for evaluation of the system [1].

Around the world, billions of people access the internet today. Intrusion detection technology is a new generation of security technology that monitor system to avoid malicious activities. The paper consists of the literature survey of Internal Intrusion Detection System (IIDS) and Intrusion Detection System (IDS) that uses various data mining and forensic techniques algorithms for the system to work in real time. Data mining methods are proposed for cyber analytics in support of intrusion detection [2].

The conventional intrusion prevention techniques such as firewalls, access control or encryption have failed to protect networks and systems from increasingly complicated attacks and malwares. As a result, Intrusion Detection System (IDS) proposed have become an essential element of security infrastructure which is useful to detect, identify these threats and track the intruders. Since then, many research works have been focused on, how to effectively and accurately construct detection models[3-5].

As the existing intrusion detection systems require input from human which is expensive to determine effective models for normal behavior, learning algorithms can be used as an alternative to discover appropriate behavior as normal and attack. Recently, there has been an increased interest in data mining-based approaches to build intrusion detection models [6]. Hence accurate intrusion detection model can be built by choosing an effective classification approach. Most of the researchers conduct experiments on the most popular benchmark dataset, Knowledge Discovery and Data Mining – KDD'99. (IDS) Intrusion Detection System is software or hardware components that automate the intrusion detection process. IDS designed to monitor the events occurring in a network and computer system and responds to events with sign of possible incidents of violations of security policies and rules [7].

Characteristics of Intrusion Detection System

There are many characteristics of the intrusion detection system that controls the specification and the networking of the system in the protection of the computer networking [8-12]. Some of the important characters are as follows:

1. A true intrusion detection system can be able to manage the security measures and can also manage all the events of the administration.
2. Several forms of intrusion detection system have the ability to detect the problem and can stop them at the spot and restrict it from succeeding.
3. Intrusion detection system also has property to that they can change the settings of the windows firewall according to this work and prevent the system from dangerous attacks.

IDS FUNCTIONS:

The functions of IDS are:

- ✓ Monitoring users and system activity.
- ✓ Auditing system configuration for vulnerabilities and miss-configurations.
- ✓ Extracting the integrity of critical system and data files.
- ✓ Recognizing known attack patterns in system activity.
- ✓ Identifying abnormal activity through statistical analysis.
- ✓ Managing audit trails and highlighting user violation of policy or normal activity.
- ✓ System configuration errors are corrected.

II. RELATED WORK

[1] In this Article, An intrusion-detection model anomaly based introduced, Classification accuracy in intrusion detection systems (IDSs) deals with such fundamental problems as how to compare two or more IDSs, how to evaluate the performance of an IDS, and how to determine the best configuration of the IDS.

[2] In this Article survey of internal IDS covered, Data mining-based intrusion detectors, the basic task in intrusion detection system is to classify network activities as normal or abnormal while minimizing misclassification. various machine learning and data mining approaches have been applied to Intrusion Detection Systems (IDSs) to protect the special computer systems, sensitive traffics cyber-attacks for computer networks. In addition, Support Vector Machine (SVM) is applied as the classification techniques in literature.

[3] In this Article an intelligent control system introduced .study explains that presently it is very important to sustain a high level security to ensure safe and trusted communication of information between many organizations.

[4] In this Article mobile agent based intrusion detection system and intrusion prevention system: a comparative study, It is explained that the Network intrusion detection systems (NIDS) are becoming an important tool for protecting critical information and infrastructure.

[5] In this Article J48 classifier based Intrusion Detection System has been deployed.

[6] In this Article multi agent based Intrusion Detection System Issues and Challenges in Anomaly Intrusion Detection with MANET concepts.

[7] In this Article host based MANET system introduced, here an Introduction to Intrusion Detection, Given NIDS performance is shown to be memory-bound, improving the cache behaviour of pattern matching techniques is a promising approach in system.

[8] In this Article, Computer security and intrusion detection, the basic goal of IDS is detecting suspicious traffic in different ways, in spite of that it comes with various approaches. Here Agentauro system has been introduced.

[9] In Article, "A Short Survey of Intrusion Detection Systems", Problems of Engineering Cybernetics and Robotics, with the dramatically development of internet, Security of network traffic is becoming a major issue of computer network system. Attacks on the network are increasing day-by-day.

[10] In this Article A Framework for the Evaluation of Intrusion Detection Systems, Intrusion detection mechanisms play a crucial role in the security landscape of an organization.

III. EXISTING METHODOLOGY & TOOLS

The most important purpose of intrusion detection system is to identify attacks against information systems. It is a security method attempting to identify various attacks. In this paper, we reviewed snort as misuse based intrusion detection system as well as ALAD, PHAD, LERAD, NETAD as anomaly based statistical algorithms [3]. There are already so many methodologies existing for Intrusion Detection System. Here I have tried to represent a conclusive methodology of IDS in Figure 1 below:

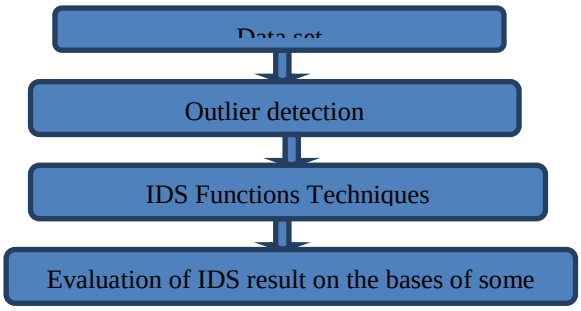

Figure 1: IDS Methodology

MATLAB:

The tool which is to be used for the implementation of the proposed work is MATLAB. The name MATLAB stands for MATrixLABoratory. MATLAB was written originally to provide easy access to matrix software developed by the LINPACK (linear system package) and EISPACK (Eigen system package) projects.

MATLAB [14-15] is a high-performance language for technical computing. It integrates computation, visualization, and programming environment. Furthermore, MATLAB is a modern programming language environment: it has sophisticated data structures, contains built-in editing and debugging tools, and supports object-oriented programming. These factors make MATLAB an excellent tool for teaching and research.

WEKA:
WEKA implements algorithms for data pre-processing, classification, regression, clustering, association rules; it also includes a visualization tools[13].

SNORT:
It is the most widely deployed intrusion prevention technology in the world. Snort can perform protocol analysis and content searching [8].

Fail2Ban:

It is host based intrusion detection system ty tool which is compatible with LINUX, UNIX, MAC-OS etc.

IV. PERFORMANCE METRICS

False Alarms: It is an event that is not supposed to be occurring in implementation.

False Negative: It occurs when attack traffic does not trigger an alert on the IDS device.

False Positive: An alert has been triggered, but it was for traffic that does not constitute an actual attack.

True Alarms: It is response of IDS.

True Negative: It is non-offending or benign traffic did not trigger an alarm.

True Positive: A true positive means that the IDS device recognized and responded to an attack.

Vulnerability: It compromises the security or functionality of a particular system in your network.

V. CONCLUSION AND FUTURE SCOPE

I have study various literature on the topic and after studying all the literature I land up with following things. At the other end Genetic algorithm is also used to reduce the data size and make more effective data aggregation. Secondly message, Introduction Detection gives security to enhance the overall security level of the data. So finally, An Effective Intrusion Detection Scheme is recommended at the point of time.

REFERENCES

[1] Roshan Kumar, Deepak SharmaHyINT: Signature-Anomaly Intrusion Detection System 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) 2018.

[2] A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS) IEEE 2017.

[3] Akash Garg ; Prachi Maheshwari,10th International Conference on Intelligent Systems and Control (ISCO), 2016.

[4] Chaimae Saadi ,Ensak-Morroco and Habiba Chaoui "Intrusion detection system based interaction on mobile agents and clust-density algorithm "IDS-AM-Clust", International Colloquium on Information Science and Technology (CiSt),IEEE,2016.

[5] ShailendraSahu and B M Mehtre ,"Network Intrusion Detection System Using J48 Decision Tree," 2015 IEEE.

[6] Sara Chadli,Mohamed Emharraf and Mohammed Saber "The design of an IDS architecture for MANET based on multi-agent" International Colloquium on Information Science and Technology (CiSt),IEEE,2014.

[7] Difan Zhang, Linqiang Ge, Rommie Hardy, Authersi Yu, Hanlin Zhang and Robert Reschly, "On Effective Data Aggregation Techniques In Host-based Intrusion Detection in MANET," The 10th Annual IEEE CCNC- Green Communications and Computations Track 2013 IEEE.

[8] Jitendra S Rathore, Praneet Saurabh, Bhupendra Verma "AgentOuro: A Novelty Based Intrusion Detection and Prevention System" Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on 3-5 Nov. 2012.

[9] Akthar, F. and Hahne, C. Rapid Miner 5 Operator Reference, 2012.

[10] Bin Zeng , Lu Yao and ZhiChen Chen"A network intrusion detection system with the snooping agents",International Conference on Computer Application and System Modeling, 2010.

[11] Vera Marinova-Boncheva, "A Short Survey of Intrusion Detection Systems", Problems of Engineering Cybernetics and Robotics, 2007.

[12] Khaled Labib, Computer security and intrusion detection, Crossroads, Volume 11, Issue 1, August 2004.

[13] Murthy, S.K. , Automatic Construction of Decision Trees from Data: A Multi-Disciplinary Survey. Data Mining and Knowledge Discovery, 24, 1998.

[14] Aurobindo Sundaram, An Introduction to Intrusion Detection, Crossroads, Volume 2, Issue 4, Pages: 3 –7, 1996.

[15] Northcutt, S. "Network Intrusion Detection: An Analyst's Handbook." New Riders, Indianapolis 1999.

Authors Profile

Mr.K.Shukla is pursuing Master of Technology in Computer Science & Engineering Department of Sarvepalli Radhakrishnan University, Bhopal (MP). He focuses on the field of computer security to strengthen computer security learning and importance.

Mr.R.K.Gupta is a well known Professor of Computer Science & Engineering Department of Sarvepalli Rdhakrishnan University, Bhopal (MP). He is pursuing Ph.D. in Computer Science from Barkatullah University Bhopal. His research interest and specialization falls upon intrusion Detection System and various Computer Security Strategies.

Dr.V.Namdeo Head of Computer Science & Engineering Department of Sarvepalli Radhakrishnan of Sarvepalli Rdhakrishnan University, Bhopal (MP). She is equiped with huge knowledge and experience of various fields of Computer Science fields.

