INTERNATIONAL JOURNAL OF TECHO-ENGINEERING

ISSN : 2057-5688

ANOMALY OF INTRUSION DETECTION A SURVEY

[1]UNDADI SWATHI, [2]M UDAY KUMAR

[1] M. Tech Scholar,[2]Associate Professor, Department of CSE,

JNTUH UNIVERSITY COLLEGE OF ENGINERING, JAGTIAL, T.S., INDIA.

Abstract: An intrusion detection system (IDS), hardware or software, is a monitoring system that monitors network and system activity to detect malicious signs. A robust intrusion detection system is a fundamental problem in computer security. It detects intrusions and alerts users when they attempt to intrude. These techniques will alert the system administrator if IDS detects intrusion. The problem of anomaly detection has been studied in many research areas. This survey attempts to give a comprehensive and structured overview of research on anomaly detection. Each technique has its own strengths and weaknesses. This review will examine the current state of experiment practice in the area of anomaly-based intrusion prevention and recent research in this field. This survey examines the current state of anomaly detection techniques and how they can be used in other areas.

Keywords: Clustering, data mining, intrusion detection system, network security.

1. INTRODUCTION:

Intrusion detection devices (IDSs), which are surveillance devices, have been added to security walls to protect against malicious activity. Network intrusion detector systems (NIDSs), are the main focus of this research. They can detect more attacks than other types of IDSs. Network IDSs examine traffic to detect ongoing and incoming attacks. To detect attacks on a network, or on a host, commercial IDSs typically use a collection of rules known as signatures. Intrusion detection system are monitoring devices used to detect intrusions in a computer network or on a computer. Christopher Kruegel, et al. define intrusions as illegal and unusual activities. A malicious adversary performs a series of related activities that result in the compromise and destruction of a target network." [1]. Network administrators are

ISSN : 2057-5688

dependent on an intrusion detection tool because it is impossible to analyse the enormous amount of packets moving through current networks every second without one. This field has seen extensive research over the past thirty years, and there are still many questions to be answered about its accuracy. You may also be able to pass the system through variants of existing attacks or new attacks without being detected[2].

An IDS functions in the same manner as an alarm, with some devices being more advanced or intelligent than others. You need to take into account many factors when creating an IDS, including data collection and data pre-processing. Intrusion recognition is the central issue. Audit data is examined and compared to detection models[3]. These models describe intrusive or benign patterns so that both successful, and unsuccessful, intrusion attempts are identified. Many intrusion detection system have been implemented in wired networks. This means that all traffic must pass through switches, routers, gateways.

The IoT security enhancement projects include access control, data confidentiality, authentication, privacy, trust, and enforcement privacy policies. Even with these measures, IoT network are still vulnerable to multiple attack attempts to disable the network[4,5]. An additional defence line is necessary to detect attackers. Intrusion Detection Systems are used to accomplish this.

IDS is one of many tools that are used to protect information systems and traditional networks. IDS monitors the network or host and alerts the administrator when it detects security violations. Since the 1980s, research efforts on intrusion detection began. His seminal work on network security monitoring was published. The IDS is a well-known defence technology for traditional IP networks. There are many solutions available[6].

.

2. REVIEW ON OBJECT DETECTION IN COMPUTER VISION COMMUNITY

Based on data collection methods and classifications, intrusion detection devices can be classified into two groups: network-based and host-based. A network-based intrusion identification system (NIDS), uses network traffic to monitor and analyse data to protect a computer system against network-based attack. Host-based intrusion

ISSN : 2057-5688

detection system (HIDS), monitors, analyses and reports data from the system log files. You can also classify intrusion detector systems based on their intrusion detection technique into three categories, misuse- detection (specification-based detection), and anomaly–based detection[7].

2.1. Signature based detection

A Signature-based Intrusion Detection Systems uses a collection of previously discovered attack signatures. They include patterns, known malicious order sequences, byte sequencing in network traffic and system vulnerabilities. Each intrusion gives a specific malicious signature such as failed logins, failed attempt to run an application, failed file and folder access and nature of data packets. Signature-based intrusion prevention system uses these signatures for detection and prevention of future attacks. The best thing about signature-based intrusion discovery system is its simplicity of development and understanding. This is because we can see the behaviour of network traffic as well as system activity. Signature-based intrusion discovery system can be used to exploit specific buffer-overflow vulnerabilities[8]. Modern systems make pattern matching easier and more efficient with less computational complexity. For example, if the system has limited communication capabilities (e.g., DNS, ICMP, SMTP), it can enable signatures that are relevant and disable those of other signatures.

2.2. Anomaly based detection

An anomaly-based Intrusion Detection System (IDS), refers to a baseline or learned pattern in normal system activity to detect active intrusion attempts. Any deviations from the pattern or baseline will trigger an alarm. Anomaly detection engines detect any behaviour that is not consistent with the accepted pattern of behaviour. Anomaly detection systems have a problem with defining rules. Every protocol that is being analysed needs to be clearly defined, implemented, and verified for accuracy. Variations in vendor implementations can also complicate the rule-defining process for different protocols. It takes a lot of effort to define rules in custom protocols. For detection to work correctly, it is necessary to collect and maintain detailed information about normal network behaviour. Once the protocol rules have been

ISSN : 2057-5688

established and the behaviour has been defined, the system scales faster than the signature-based model[9,10]. This makes it more useful for anomaly detection. If malicious behavior is not considered normal usage, it can go unnoticed. A directory traversal activity using server that complies with network protocol does not trigger any bandwidth limit flags, payload flags, or other flags. Anomaly detection is more effective than signature-based systems for detecting new automated worms. If an attack falls outside of normal traffic patterns, it can be detected. A worm infects a system and starts to scan for other vulnerable systems. This floods the network at an abnormal rate, causing a network bandwidth abnormality rule. An alarm is raised if the computer system exhibits abnormal behavior or intrusive activity that is not normal[11]. This is why there is a continuous monitoring.

3. TYPES OF INTRUSION DETECTION SYSTEMS

According to analytic methods, Intrusion Detection System can also be classified into two types: Abnormal Detection and Misuse Detection.

A. Anomaly Detection

Anomaly systems use the opposite approach. They first know what normal is and then look for deviations from that normal behavior. These deviations can be referred to as possible intrusions or anomalies. To detect anomalies, anomaly detection systems use knowledge of normal behavior. Attacks, even new ones, are detected as long the behavior is sufficiently different from normal. It is possible that the attack may not be detected if it is identical to normal behavior. It is also difficult to link specific attacks with deviations. Normal behavior should be redefined as users alter their behavior[12].

B. Misuse detection

To detect misuse, misuse detection systems use prior knowledge of attacks to search for attack traces. They detect intrusions by identifying the misuse [2]. The most

ISSN : 2057-5688

popular examples of misuse detection systems are those that use signature (or rule)-based systems. Signature-based detection seeks attack signatures in the monitored resource. Signature-based detection systems are very precise on known attacks that are contained in their signature database. Signatures can be easily identified because they are associated with particular misuse behavior. Their detection capabilities are limited to signature databases. A signature database must be continuously updated to reflect new attack signatures as they are discovered[13].

Intrusion detection is the creation of a system that automatically scans network activity to detect attacks. The system administrator can be notified if an attack is detected and take appropriate action[14].

Generally, there are four categories of attacks . They are:

1. DoS (Denial of Service) – trying to prevent a legitimate user from accessing the service in the target machine.

2. Probe – scanning a target machine for information about potential vulnerabilities.

3. R2L (Remote to Local) – when attacker attempts to obtain non-authorized access into a machine or network.

4. U2R (User to Root) – when target machine is already invaded, but the attacker attempts to gain access with super-user privileges.

Machine learning based on detection. The system will improve its performance by using previous results. It means that machine-learning gives a system the ability to enhance execution strategies. Although machine learning can be used in many different applications, these systems are costly. Machine learning techniques can be used in many different applications. They use methods that are similar to those of data mining techniques and statistical techniques. Machine learning techniques can be classified as Neural networks and Fuzzy logic approaches, Support vector machines, or Neural networks. Neural Networks machine learning techniques use neural network concepts. These concepts allow the user to anticipate for the next commands

ISSN : 2057-5688

using the sequences of commands. The neural network model does not require user behavior information[15]. Signature matching system is a highly efficient method of using a trained neural network that includes back propagation, feed forward mechanism, and a well-trained neural model.

Multilayer Perceptrons, Radial Basis functionBasedneural networks can be used to detect anomalies. IDS using neural network has three phases. To gather enough training data, the audit log is analysed in the first phase. Next, the neural network is trained to understand each user's behavior. To detect suspicious behavior, each user's behavior is compared with data[15].

4. RESEARCH CHALLENGES

Any organization should have an Intrusion Detection System. There are many researches underway to improve IDS technology. IDS technology has become highly automated. If there are any malicious actions, the IDS will notify the administrator. The administrator can then take appropriate steps to prevent future attacks. It is important to maintain logs of IDS activity. These logs can be analyzed regularly. It is essential to establish baseline policies in order to implement efficient IDS systems and reduce false alarm rates. False positive results are a common problem with intrusion detection systems[16]. Researches are ongoing to develop real-time intrusion detection systems using virtualization technologies. Virtualization technologies can handle many aspects of an intrusion detection system. Virtualization is customizable in most cases. Host-based intrusion detection systems make use of the latest development in real-time intrusion detection system[17].

The main challenge in intrusion detection systems is to reduce memory and computational power consumption. Despite many improvements to intrusion detection system, false negative rates are still too high for many applications. IDS is an integral part of intrusion detection systems. IDS is a mechanism that detects attacks, prevents malicious activity and restores the system to a secure state. If the inputs are not semantically balanced, IDSs will require more manual input to reduce false positive alarm rates[18]. It can stop attacks such as outgoing denial of service attacks

ISSN : 2057-5688

if IDS is well designed. If the IDS detects denial-of service attacks, it alerts the administrator. For detecting malicious activity within the host system, the IDS uses the data traces as well as the basic system properties.

IDS can be part of large intrusion detection systems and act as a source for basic information. Designing an efficient, self-learning IDS is a significant challenge in the intrusion detection domain. It is necessary to further research the development of an IDS that uses trusted platform modules and cryptographic technology. A smart phone and tablet intrusion detection system is another major challenge. It is difficult to provide a high intrusion detection rate in an operating system compromised. The IDS must be able to work independently in a shared system environment as the shared parameters could cause an attack. Attacks can affect the IDS' ability to quickly recover from an attack. Virtual machine is used to monitor various processes and events in IDS[19,20].

5. CONLUSION

This paper aims to give an overview of the various aspects of an anomaly-based host intrusion detection system. IDS play a significant role in many intrusion detection systems. We have reviewed the merits and disadvantages of various methods for anomaly detection. The results of IDS using various data mining algorithms and cluster-based approaches are more accurate with lower false alarm rates. A hybrid solution that combines network-based and host-based IDSs can be used in many application domains. Organizations have different requirements when choosing intrusion detection systems. The survey covered multiple approaches to the problem of anomaly detection. A better understanding of the various types of anomalies will allow for better intrusion detection systems. The anomaly detection field has many promising research directions. However, most anomaly detection methods require large amounts of test data to detect anomalies. The main directions for research in anomaly detection include the development of efficient anomaly detection methods that work with complex systems (e.g., aircraft system) and the interaction between different components in real-time.

ISSN : 2057-5688

REFERENCES:

[1] Syed ShariyarMurtaza, WaelKhreich, AbdelwahabHamou-Lhadj and Stephane Gagnon 2015 A trace abstraction approach for host-based anomaly detection Computational Intelligence for Security and Defense Applications (CISDA) pp. 1-8

[2] Bukac V., Tucek P and Deutsch M. 2012 Advances and Challenges in Standalone Host-Based Intrusion Detection Systems. In: Fischer-Hübner S., Katsikas S., Quirchmayr G. (eds) Trust, Privacy and Security in Digital Business. TrustBus

[3] V. Jyothsna and V. V. Rama Prasad 2011 A Review of Anomaly based IntrusionDetection Systems International Journal of Computer Applications vol 28

[4] Jiankun Hu and Xinghuo Yu 2009 A Simple and Efficient Hidden Markov Model Scheme for Host-Based Anomaly Intrusion Detection IEEE Network Journal vol. 23

[5] DavoodKheyri and MojtabaKarami 2012 A Comprehensive Survey on Anomaly-Based Intrusion Detection in MANET Computer and Information Sciencevol. 5

[6] Asmaa A and Sharad G 2011Importance of Intrusion Detection System (IDS) International Journal of Scientific & Engineering Researchvol.2

[7] Parvathi Devi and Siva Prasad 2012 Study of Anomaly Identification Techniques in Large Scale SystemsInternational Journal of Computer Trends and Technologyvol.3

[8] Varun C, Arindam B and Vipin K 2009 Anomaly Detection: A Survey ACM Computing Surveysvol. 41

[9] Gideon Creech and Jiankun Hu. 2014 A semantic approach to host-based intrusion detection systems using contiguousanddiscontiguous system call patternsIEEE Transactions on Computers vol63 pp 807–819

[10] XuanDau Hoang, Jiankun Hu, and Peter Bertok 2003 A multi-layer model for anomaly intrusion detection using program sequences of system calls. In Proc. 11th IEEE Intl. Conf. Citeseer

ISSN : 2057-5688

[11] Lokendra Singh Parihar and AkhileshTiwari 2016 Survey on Intrusion Detection Using Data Mining Methods International Journal for Science and Advance Research in Technology, vol 2

[12] Kymie Tan and Roy A Maxion 2003 Determining the operational limits of an anomaly-based intrusion detectorIEEE Journal on Selected Areas in Communicationsvol 21 pp 96–110

[13] Christina Warrender, Stephanie Forrest, and Barak Pearlmutter 1999 Detecting intrusions using system calls: Alternative data models.Proceedings of the 1999 IEEE Symposium on Security and Privacypp 133–145

[14] Qayyum, A.; Islam, M.H.; Jamil, M 2005 Taxonomy of statistical based anomaly detection techniques for intrusion detectionProceedings of the IEEE Symposium on Emerging Technologies pp 17-18

[15] ShikhaAgrawal and JitendraAgrawal 2015 Survey on Anomaly Detection using Data Mining Techniques Procedia Computer Science, vol 60 pp 708-713

[16] James C and Jay HA 1996 Comparative Analysis of Current Intrusion Detection TechnologiesProceedings of Technology in Information Security Conference (TISC), pp. 212-218

[17] Dorothy D 1987 An Intrusion-Detection Model IEEE Transactions on Software Engineeringvol13 pp. 222, 232

[18] Vasilios S and Fotini P 2006 Application of anomaly detection algorithms for detecting SYN flooding attacksElsevier, Computer Communications vol. 29 pp 1433, 1442

[19] Li Yang and Guo Li 2007 An active learning based TCMKNN algorithm for supervised network intrusiondetection, Elsevier, Computers & Security pp 459–467

[20] Garcia-Teodoro, Pedro, J. Diaz-Verdejo, Gabriel M and Enrique V 2009Anomaly-based network intrusion detection: Techniques, systems and challengescomputers & securityvol 28 pp 18, 28