ACTA TEHNICA CORVINIENSIS – Bulletin of Engineering
Tome VIII [2015] Fascicule 1 [January – March]
ISSN: 2067 – 3809

[1.] Sugata SANYAL, [2.] Niva DAS, [3.] Tanmoy SARKAR

SURVEY ON HOST AND NETWORK BASED INTRUSION DETECTION SYSTEM

[1.] Corporate Technology Office, Tata Consultancy Services, Mumbai, INDIA
[2.] University of Calcutta, Kolkata, INDIA
[3.] Neudesic India Pvt. Limited, Hyderabad, INDIA

Abstract: With invent of new technologies and devices, Intrusion has become an area of concern because of security issues, in the ever growing area of cyber-attack. An intrusion detection system (IDS) is defined as a device or software application which monitors system or network activities for malicious activities or policy violations. It produces reports to a management station. In this paper we are mainly focused on different IDS concepts based on Host and Network systems.

Keywords: Intrusion, Intrusion Detection System (IDS), Host based Intrusion Detection System (HIDS); Network based Intrusion Detection System (NIDS)

INTRODUCTION

With the recent advances in technology, people are sharing more and more information among each other. Some organizations like medicine, military etc. are sharing data which is highly sensitive and important. For secure communication, people are using cryptography, using secret key, so that only authenticated receiver can decrypt the message and authenticity of message remains intact. But intruders are not interested to decrypt message. They can use sophisticated tools to attack the host on the network and get access to the sensitive data. Here, IDS comes as a savior. IDS provide three important security functions of monitoring, detecting and responding to unauthorized activities [2]. It usually provides three services: Observing and analyzing the host and the network activities, audit system configurations and evaluating of integrity of critical information by estimating abnormal activities. IDS are generally classified as follows:

1. Host-Based (HIDS): Host based intrusion detection systems run on individual hosts / devices on the network. It monitors the incoming and outgoing packets from the device and alerts the administrator on detection of suspicious activity.
2. Network-Based (NIDS): Network based intrusion detection systems monitor traffic between all devices on the network. On performing an analysis for a passing traffic on the entire subnet (in a promiscuous mode), it subsequently matches the traffic on the subnets to the collection of known attacks. On finding a match, alert is sent to the administrator. Today, IDS becomes necessary for every organization to secure their sensitive data from intruders. In the next sections, we will discuss about various tools and techniques used in Host based and Network based Intrusion detection systems.

HOST BASED IDS

Host based IDS is aimed at collection and analysis of information on a particular host or system [3]. This Host agent monitors and prevents intruders to compromise system security policy. HIDS plays different role from Anti-virus. Anti-virus is supposed to monitor all the activities inside the system but not concerned with buffer overflow attacks on system memory nor malicious behavior of operating system process but HIDS checks and collect system data including File System, Network Events, System Calls to verify whether any inconsistency has occurred or not. HIDS system relies heavily on audit trail and system logs to detect unusual activities inside the system. Host-based systems can monitor access to user specific information which is a major advantage [3], [4]. HIDS can identify an improper user of company resources. On detection of similar pattern (similar to past attacks or suggestive of an attack); activity with that workstation can be stopped, thus blocking the attack. This is greatly useful in systems where system resources are accessed remotely in a routine manner. Some major disadvantages as follows:

(1) they cannot see the network traffic [3];

(2) HIDS rely heavily on audit trails which can exhaust a lot of resource and space in server, and

(3) lack of cross-platform interoperability.

Inspection of system configuration files to check for failure-prone setting and of other system objects for security policy violations are the basic job of a HIDS host-based mechanism [3]. If intruders succeed in modifying the HIDS itself then there is no way to detect intrusion – unless security administrators take appropriate precautions.

ELM Enterprise Manager [6], an enterprise class event log management solution, collects event logs from different devices in

real-time. On detection of critical events, immediate email alerts are helpful in activating more stringent security policies.

[8] has proposed an Intrusion Detection System where they compare the performance of their fuzzy rule based classifiers for IDS with similar performance obtained from the decision tree, support vector mechanisms and linear genetic programming. Toosi et al. [9] presented a method to classify the normal and abnormal behavior in network, proposing Adaptive Neuro Fuzzy Inference system to categorize normal and suspicious behavior and detect intrusion.

Abraham et al. [10] have proposed an Intrusion Detection System which uses Distributed IDS to detect intrusion in a network. The approach makes use of three fuzzy rule based classifiers in a distributed environment to detect intrusion detection.

David et al [28] introduce concept of mimicry attack which allows an advanced intruder to hide their identification to avoid IDS detection. The authors then propose theoretical concept to detect and prevent mimicry attacks.

Yeung et al [29] adopt an anomaly detection approach. They detect possible intrusions, based on program or user profiles, built from normal usage data. Here the dynamic modeling approach, based on Hidden Markov Models (HMM) and the static modeling approach, based on event occurrence frequency distribution have been extensively used.

STATL is a state/transition based attack description language, which is extensible. This is developed by Eckmann et al [30]. It is intended to describe intrusion detection type activity. A STATL helps describe both domain-independent attacks and for providing constructs to help extending the language. This is for taking care of attacks to particular domain and environments.

NETWORK BASED IDS

Network Based Intrusion Detection Systems (NIDS) are active systems. These are deployed on networks to primarily monitor the network traffic. NIDS are operated under promiscuous mode without exposing itself to the potential attackers. NIDS systems generally work by identifying attacking signature within the networks. NIDS are OS independent and also compromising one NIDS will not affect the system if multiple NIDS are deployed to monitor the traffic flow. Sometimes network people raise a question like what can NIDS do that Firewall can't? The firewall is the equivalent of a security fence around a property and the guard post at the front gate. But Firewall is not able to detect what is happing inside [3]. Firewalls are subject to many attacks, tunneling attacks and application-based attacks are most prominent. On the other hand a NIDS system works like a body guard which is monitoring both inside and outside of a property. It monitors packets, matches pattern; find attacking signature from already existing attacks done in the past and sometime statistical analysis of the information to detect abnormal behavior. However NIDS system cannot scan the content if network traffic is encrypted, it cannot efficiently handle high speed networks.

Snort [5], an open source network intrusion prevention system, is capable of performing real-time traffic analysis and packet logging on IP networks. It can handle various intrusion detection techniques like buffer overflow, protocol analysis, CGI attack and many more.

Trivedi et al. [7] proposed an Intrusion Detection System which defines a term called "Reputation" that is assigned to every node in the network. Every node monitors the behavior of its next-hop neighbor through promiscuous mode. A reputation manager keeps track of all the "Reputation" values from all the nodes, for updating the reputation value. A node is declared as malicious whenever it crosses a predefined threshold. A warning message is sent only to the immediate neighbors. Each node also contains an Avoid list. It contains a list of malicious nodes and no further communication is done through these already identified malicious nodes.

Toosi et al. [11] presented a method to classify the normal and the intrusive behavior in a network. They used a combination of neuro-fuzzy networks, fuzzy interference and genetic algorithm to classify the network. Parallel neuro-fuzzy classifiers did the initial classification and its output was the basis of the fuzzy inference system. Finally, the genetic algorithm approach was used to optimize the decision.

Faysel and Haque [12] surveyed various methods of cyber-attack detection and classification technique. These are based on neural networks and data mining. They have also discussed IDS evaluation criteria and dataset for IDS validation. Trivedi et al. [13] suggested a Semi Distributed Reputation-based IDS method for Mobile Ad Hoc Networks (MANETs) proposing a unique concept of redemption and fading with path manager and monitor system, making the system invulnerable to many MANET attacks. An Ant Colony based IDS was proposed by Banerjee et al. [14] which keeps track of the intruder trails and works in conjunction with the machine learning system to make sensor networks less vulnerable to intrusion attacks. Saravanakumar et al. [15] tackle the issue of complexity and throughput, prime important points in the current Intrusion Detection Systems (IDS). They compare various IDS systems that use different algorithms to detect the intrusions. They proposed a scheme that uses a combination of Artificial Neural Network algorithms to design IDS. This enables faster convergence and delivers better performance.

Shun and Malki [16] have a scheme which uses feed forward neural networks with back propagation training to predict and detect the attacks on network. With appropriate training the proposed IDS system greatly enhances the performance of the IDS system and detects the known and unknown attacks with higher probability. Intrusion Detection System (IDS), developed by Chavan et al. [17], uses Fuzzy Inference System and Artificial Neural Networks and it is trained by creating a signature pattern database, using Protocol Analysis and Neuro-fuzzy learning method.

Dal et al. [18] proposed an Intrusion Detection System method which applies Genetic Algorithm with Artificial Immune System (AIS). They have evolved a Primary Response following the concept of memory cells which is dominant in Natural Immune System, enabling faster

detection of already encountered attacks. These cells are random in nature, dependent on the evolution of the detectors, thus granting greater immunity from anomalies and attacks.

Dasgupta et al. [19] focuses on the recent improvements in Artificial Immune System [AIS]. Yang et al. [20] use a related method in AIS to enhance the performance of IDS, using antibody concentration to evaluate the damaging power of the intrusion in the network.

Hosseinpour et al. [21] suggested a method to improve the detection performance and accuracy of IDS system, proposing a distributed multilayered framework to improve the detection and efficiency of IDS. The genetic algorithm proposed by them enhances the secondary immune response of the system.

Jie et al. [22] devised a method for signal detection using Artificial Immune System [AIS] for anomalistic signal detection in an electromagnetic environment. Saboori et al. [23] proposed an Apriori Algorithm to detect an anomaly in the system. It predicts a novel attack and generates a set of real-time rules for the firewall, and functions by extracting the correlation relationships among large data sets.

Nikolova and Jecheva [24] suggested an anomaly based Intrusion Detection System (IDS) using data mining techniques like classification trees to describe the normal activity of the system. Similarity coefficients are used to detect the intrusion in the system, which compare the similarity between the normal behavior and the observed behavior. Depending on the measured degree of similarity, a decision is reached about the system being under attack or not.

Karim [25] described application of Computer Intelligence in the Network Intrusion Detection, explaining the usage of clustering, feature selection, and anomaly detection.

Jianhua et al. [26] describes detection and exclusion of misbehaving nodes by dropping packets forwarded through them. A reputation-based scheme for efficiently solving the problem has been suggested where nodes with bad comprehensive reputation will be excluded from the network.

Thakur et al [27] described a multi-dimensional approach towards intrusion detection. Network and system usage parameters like source and destination IP addresses, ports; incoming and outgoing network traffic data rate and number of CPU cycles per request are divided into multiple dimensions. Authors established a conditional function during the training phase for each dimension.

CONCLUSION

Network-based and host-based IDS prevent both insider as well as outsider attacks. There are ever evolving methods of intrusion detection but most systems utilize signatures to search for patterns of misuse and either automatically respond to the misuse or intimates system administrator to take appropriate action. Some intrusion detection systems even sense misappropriation by using behavioral data forensics. Due to inherent risk of some automated responses, there is still need for human intervention that can supervise and ensure the state of the system.

REFERENCES

[1.] http://en.wikipedia.org/wiki/Intrusion_detection_system
[2.] Defeng Wang, Yeung, D.S., and Tsang, E.C., "Weighted Mahalanobis Distance Kernels for Support Vector Machines", IEEE Transactions on Neural Networks, Vol. 18, No. 5, Pp. 1453-1462, 2007
[3.] Bace, Rebecca: An Introduction to Intrusion Detection & Assessment. Infidel Inc., prepared for ICSA Inc. Copyright 1998.
[4.] Brackney, R: Cyber-Intrusion Response. Proceedings of Seventeenth IEEE Symposium on Reliable Distributed Systems, West Lafayette, IN, 20-23 Oct, 1998, pp. 413-415.
[5.] Matthew Richard, "Intrusion Detection FAQ: Are there limitations of Intrusion Signatures?" http://www.sans.org/security-resources/idfaq/limitations.php, April 5, 2001.
[6.] "Comprehensive Windows Event Log Monitoring - Servers, Desktops & Devices", http://www.tntsoftware.com/, June 12, 2014.
[7.] Animesh Trivedi, Rishi Kapoor, Rajan Arora, Sudip Sanyal, Sugata Sanyal, "RISM - Reputation Based Intrusion Detection System for Mobile Ad hoc Networks", Third International Conference on Computers and Devices for Communication (CODEC-06), Institute of Radio Physics and Electronics, University of Calcutta, December 18-20, 2006, pp. 234-237.
[8.] Ajith Abraham, Ravi Jain, Sugata Sanyal, Sang Yong Han, "SCIDS: A Soft Computing Intrusion Detection System", 6th International Workshop on Distributed Computing (IWDC-2004), Springer Verlag, Germany, Lecture Notes in Computer Science, Vol. 3326. 2004, pp. 252-257
[9.] A. N. Toosi, M. Kahani, R. Monsefi, "Network Intrusion Detection based on Neuro-fuzzy classification," International Conference on Computing & Informatics, (ICOCI '06), Kuala Lumpur, Malaysia, June 6-8, 2006, pp. 1-5.
[10.] Ajith Abraham, Ravi Jain, Johnson Thomas, and Sang Yong Han. "D-SCIDS: Distributed soft computing intrusion detection system." Journal of Network and Computer Applications 30, no. 1 (2007): 81-98.
[11.] A. N. Toosi, M. Kahani. "A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers." Computer Communications 30, no. 10 (2007): 2201-2212.
[12.] Mohammad A. Faysel, Syed S. Haque, "Towards Cyber Defense: Research in Intrusion Detection and Intrusion Prevention Systems", IJCSNS International Journal of Computer Science and Network Security, Vol.10 No.7, July 2010, pp. 316-325.
[13.] Animesh K Trivedi, Rajan Arora, Rishi Kapoor, Sudip Sanyal, Sugata Sanyal, "A Semi-distributed Reputation-based Intrusion Detection System for Mobile Ad hoc Networks", Journal of Information Assurance and Security (JIAS), Volume 1, Issue 4, Dec. 2006, pp. 265-274.
[14.] S. Banerjee, C. Grosan, A. Abraham, P. K. Mahanti, "Intrusion detection in sensor networks using emotional ants," Proceedings of 5th International Conference on Intelligent Systems Design and Applications, (ISDA '05), Wroclaw, Poland, Sept. 8-10, 2005, pp. 344-349.
[15.] S. Saravana Kumar, Umamaheswari, D. Jayalakshmi, R. Sugumar, "Development and implementation of artificial neural networks for intrusion detection in computer network", IJCSNS: Int. Journal of

Computer Science and Network Security. 2010. vol. 10, No. 7, pp. 271-275.

[16.] Jimmy Shun and Heidar A. Malki, "Network Intrusion Detection System Using Neural Networks", Fourth International Conference on Natural Computation,(ICNC '08),vol.5, Oct. 18-20, 2008, pp.242-246.

[17.] Sampada Chavan, Khusbu Shah, Neha Dave, Sanghamitra Mukherjee, Ajith Abraham, Sugata Sanyal, "Adaptive Neuro-Fuzzy Intrusion Detection Systems", IEEE International Conference on Information Technology: Coding andComputing,2004 (ITCC '04), Proceedings of ITCC 2004, Vol. 1, 2004, Las Vegas, Nevada, pp. 70-74.

[18.] Divyata Dal, Siby Abraham, Ajith Abraham, Sugata Sanyal, Mukund Sanglikar, "Evolution Induced Secondary Immunity: An Artificial Immune System based Intrusion Detection System", 7th International Conference on Computer Information Systems and Industrial Management Applications, (CISIM '08), June 26-28, 2008, pp.65-70

[19.] D. Dasgupta, S. Yu, F. Nino, "Recent Advances in Artificial Immune Systems: Models and Applications", Applied Soft Computing, Elsevier, Vol. 11, March, 2011, pp.1574-1587.

[20.] Jin Yang, Yi Liu, Jian Jun Wang, Jian Dong Zhang, Bin Li, "Dynamical Immunological Surveillance for Network Danger Evaluation Model," 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom '09), Beijing, China, Sept. 24-26, 2009, pp.1-4.

[21.] F. Hosseinpour, K. Abu Bakar, A. Hatami Hardoroudi, A. Farhang Dareshur, "Design of a new distributed model for Intrusion Detection System based on Artificial Immune System," 2010 6th International Conference on Advanced Information Management and Service (IMS), Seoul, Korea, Nov. 30-Dec. 2, 2010, pp.378-383.

[22.] MA Jie, SHI Ying-chun, ZHONG Zi-fa, LIU Xiang, "An Anomalistic Electromagnetism Signal Detection Model Based on Artificial Immune System," 2010 International Conference on Communications and Intelligence Information Security (ICCIIS), NanNing, China, Oct. 13-14, 2010,pp.256-260.

[23.] E. Saboori, S. Parsazad, Y. Sanatkhani, "Automatic firewall rules generator for anomaly detection systems with Apriori algorithm," 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, China,Vol.6, 2010, pp.V6-57-V6-60.

[24.] Evgeniya Nikolova, Veselina Jecheva, "Some similarity coefficients and application of data mining techniques to the anomaly-based IDS", Telecommunication Systems, December, 2010, Springer Netherlands, pp. 1-9.

[25.] Asim Karim, "Computational Intelligence for Network Intrusion Detection: Recent Contributions and Security", Computational Intelligence and Security, International Conference, CIS 2005, Xi an, China, December 15-19, 2005, Proceedings, Part I. Volume 3801 of Lecture Notes in Computer Science, pp. 170-175.

[26.] Song Jianhua, Ma ChuanXiang "A reputation-based scheme against malicious packet dropping for mobile ad hoc networks", IEEE International Conference on Intelligent Computing and Intelligent Systems, 2009. ICIS 2009, volume 3, 20-22 Nov. 2009, Pages 113 – 117, E-ISBN 978-1-4244-4738-1.

[27.] Manoj Rameshchandra Thakur, Sugata Sanyal, "A Multi-Dimensional approach towards Intrusion Detection System" in arXiv preprint arXiv: 1205.2340, 2012.

[28.] David Wagner, Paolo Soto "Mimicry Attacks on Host-Based Intrusion Detection Systems" CCS'02, November 18–22, 2002, Washington, DC, USA. Copyright 2002 ACM 1-58113-612-9/02/0011.

[29.] Dit-Yan Yeung, Yuxin Ding "Host based Intrusion detection using dynamic and static behavioral models", Pattern Recognition, Volume 36, Issue 1, January 2003, Pages 229-243

[30.] Steven T. Eckmann, Giovanni Vigna, Richard A. Kemmerer, "STATL: An attack language for state-based intrusion detection". Computer Science and Networking and Security, Volume 10, Number 1-2 / 2002, Pages 71-103.

ACTA Technica CORVINIENSIS
BULLETIN OF ENGINEERING
ISSN:2067-3809