The Design A Functional Intrusion Detection System Based On Anomaly Detection Technique.

Adeshipo, M.E. & Adedibu, O
Department of Electrical/Electronic Engineering
The Polytechnic, Ibadan
Ibadan, Nigeria
ibuacademy@yahoo.com

ABSTRACT

The central challenge with computer security is determining the difference between normal and potentially harmful activity. For half a century, developers have protected their systems using rules that identify and block specific events. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents. These events might be violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized. Although many incidents are malicious in nature, many others are not; for example, a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization. This research reviews the concept of intrusion, countermeasures used for preventing and detecting attacks in a LAN network. The objective is to design a functional intrusion detection system based on anomaly detection technique.

Key words: Design, Functional Intrusion Detection, System and Anomaly Detection Technique.

iSTEAMS Cross-Border Conference Proceedings Paper Citation Format
Adeshipo, M.E. & Adedibu, O (2018): The Design A Functional Intrusion Detection System Based On Anomaly Detection Technique. Proceedings of the 13th iSTEAMS Multidisciplinary Conference, University of Ghana, Legon, Accra, Ghana.
Vol. 2, Pp 295-300

1. GENERAL OVERVIEW

Alongside other techniques for preventing intrusions such as encryption and firewalls, intrusion detection systems (IDSs) are another significant method used to safeguard computer systems. (N. Jaisankar et. al 2009). A critical aspect of the security of a computer based system is to the ability to fend off potential intruders and identify actual intruders. An Intrusion Detection System (IDS) has been traditionally categorized according to the way it collects data and the detection method used on the data collected (N.Jaisankar et. al 2009). If the data processed originates from one or more hosts, then the IDS is called host-based. This methodology is mostly based on examining system logs and has become obsolete. However, if the IDS monitors a network of interconnected hosts for malicious traffic it is called network-based. Network-based intrusion detection systems are more efficient because of their ability to combine network traffic data with audit data from individual hosts. The second categorization divides IDS into anomaly detection and misuse detection systems. Anomaly detection systems monitor the system and try to decide whether its behavior is normal or not. Misuse detection systems on the other hand search for known attack signatures. A signature is a trail of a known attack.

For example, it may be a specific series of bits in the header of an IP packet. Such systems resemble in their function to anti-virus programs. A weakness of this architecture is that they have to be updated on day to day basis, by downloading new attack signatures, Chatzigiannakis, Androulidakis, Grammatikou, & Maglaris (2004). Due to huge and complex infrastructure of computer networks it is very difficult to completely secure such networks. So, an intrusion detection system (IDS) is needed. Whenever the confidentiality, integrity, and availability of computer resources are under attack, it will help to detect and respond effectively. From all such attacked nodes the evidences of intrusions have to be gathered. An intruder may move between multiple nodes in the network.

Due to this the origin of attack is concealed. This report includes the findings and the results of the thorough research performed on distributed networks with focus on LAN network attacks during the course of the project. In addition, this report contains a detailed explanation of the design and the implementation of the work done to develop an Intrusion Detection and Prevention System for a LAN network. This system is helpful to detect such intrusion activities spread over the whole network. In the following sections, we briefly introduce the areas of IDSs

2. STATEMENT OF PROBLEM

The wide spread in the use of the Local Area Network (LAN) and Wide Area Network (WAN) application areas in business, financial, industry, security and healthcare sectors made us more dependent on computer networks. All these application areas had made the network an attractive target for the abuse and a big vulnerability for the computer users. Though there are contemporary methods (firewall, encryption, antivirus) that can be employed to protect data stored within a computer system of networked computers, the ability to be able to identify instances of an attack on the computer is paramount in ensuring effective deployment of security mechanism. Intrusion detection is therefore central to the concept of computer network security. This research work is therefore aimed at discussing the current research and development efforts to detect the penetration of computer systems and networks.

3. OBJECTIVES OF THE STUDY

The objectives of the study are highlighted below:

1. To review the concept of intrusion, countermeasures used for preventing and detecting attacks in a LAN network
2. To design a functional intrusion detection system based on anomaly detection technique.

4. RESEARCH METHODOLOGY

IDS systems are sensor based networks where sensors moves round each node in the network. We will design our system such that on getting an alert, the IDS will move towards the node and resolves it by killing any process that might have been started by the intruder thereby reducing the threshold back to within range of operation. The system will be simulated using Microsoft Visual Studio 2010 IDE and Microsoft SQL SERVER. The Visual Studio provides the users with the interface while the back end is the SQL Server. C# is used to implement the design. It belongs to the .NET programming family. The .NET environment allows today's analysts and developers with robust features such as Object Oriented Programming, Interoperability, Common Runtime Engine, Language Independence and security.

5. SIGNIFICANCE OF THE STUDY

Due to the popularity of the computer networks, their connectivity and our ever growing dependency on them, realization of intrusion can have devastating consequences. Securing such an important infrastructure has become the priority one research area for many researchers. Being that IDS is still a young field of research but due to its critical nature; it has attracted a lot of interests from security experts. This research will therefore help in finding an appropriate method for protecting computers in networked environment against intrusions and also to developing an intrusion detection system that is concerned to making sure that in case of an intrusion attempt, the system is able to detect and to report it.

6. SCOPE

The focus of this research is protecting the host computers in a LAN network against intentional or unintentionally illegal intrusions.

7. ORGANIZATION OF THE STUDY

The remainder of this project is organized as follows. Chapter Two discusses the concept of intrusion, and intrusion detection and prevention techniques. Chapter three describes the development of functional intrusion detection in a LAN network. Chapter Four explains the implementation of the IDS and Chapter Five Concludes and provides necessary recommendations on future work on IDS in a LAN network

Definition of Terms

- **Alarm filtering:** The process of categorizing attack alerts produced from an IDS in order to distinguish false positives from actual attacks.
- **ArachNIDS** (Advanced Reference Archive of Current Heuristics for Network Intrusion Detection Systems)
- **Attacker** or **Intruder:** An entity which tries to find a way to gain unauthorized access to information, inflict harm or engage in other malicious activities.
- **Burglar Alert/Alarm:** A signal suggesting that a system has been or is being attacked.
- ***Database Server:***The *database server* is a repository for event information recorded by sensors, agents, and/or management servers. Many IDSs provide support for database servers.
- **DDoS** Distributed denial of service
- **Detection Rate:** The detection rate is defined as the number of intrusion instances detected by the system (True Positive) divided by the total number of intrusion instances present in the test set.
- **DIDS** - Distributed Intrusion Detection System
- **False Negative:** When no alarm is raised when an attack has taken place.[
- **False Positive:** An event signaling an IDS to produce an alarm when no attack has taken place.
- **IDES** Include Intrusion-Detection Expert System
- ***IDS core system:*** The detection system monitors several parameters to determine the correlation among the observed parameters during intrusive activities.
- **IDS** Intrusion Detection System
- ***Management Server:***The *management server* is the centralized device that receives information from the sensors and manages them.
- **MIDAS** - Multics Intrusion Detection and Alerting System
- **NADIR** - Network Anomaly Detection and Intrusion Reporter
- **NBA** - Network Behavior Analysis
- ***Sensor:***TheSensors monitors and analyze activity on the network. It communicates with the management server and IDS to report an intrusion and it is also used to resolve the intrusion.
- **Site policy:** Guidelines within an organization that control the rules and configurations of an IDS.
- **True Negative:** An event when no attack has taken place and no detection is made.
- **True Positive:** A legitimate attack which triggers an IDS to produce an alarm.
- **User Interface:** Thisis a program that provides an interface for the IDS's users and administrators.
- **VPN** Virtual private network

REFERENCES

1. Aickelin U, P Bentley, S Cayzer, J Kim, and J McLeod. Danger theory: The link between ais and ids. In *Proc. of the Second Internation Conference on Artificial Immune Systems (ICARIS-03)*, pages 147–155, 2003.
2. Anita K. Jones and Robert S. Sielken , "Computer System Intrusion Detection: A Survey", http://www.cs.virginia.edu/~jones/IDS-research/Documents/jones-sielken-survey-v11.pdf
3. Bace, R., Mell, P. 2001. Intrusion Detection Systems. Special Publication 800-31,National Institute of Standards and Technology (NIST).
4. Balasubramaniyan J.S, J. O. Garcia-Fernandez, D. Isacoff, Eugene H. Spafford, Diego Zamboni: An Architecture for Intrusion Detection Using Autonomous Agents. ACSAC 1998: 13-24
5. Biswanath Mukherjee, Todd L. Heberlein, and Karl N. Levitt, "Network Intrusion Detection", IEEE Network, May/June 1994
6. ChandrashekharA. M and K. Raghuveer (2013), "Intrusion Detection Technique by using K-means, Fuzzy Neural Network and SVM classifiers", International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, INDIA, **(2013)** January 4-6.
7. Chatzigiannakis V, G Androulidakis, M Grammatikou, B Maglaris. A distributed intrusion detection prototype using security agents, HP OpenView University Association
8. Chatzigiannakis V., Androulidakis G., Grammatikou M., Maglaris B. (2004) *"A Distributed Intrusion Detection Prototype using Security Agents"* Network Management & Optimal Design Lab (NETMODE), ECE Department – National Technical University of Athens (NTUA) Iroon Polytechniou str. Zografou, Athens, Greece.
9. Curry D. and H. Debar, "Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language(XML) Document Type Definition", Internet Draft, November 2002.
10. Dhakar M. and A. Tiwari,(2012) "A New Model for Intrusion Detection based on Reduced Error Pruning Technique" International Journal of Computer Network and Information Security, **(2013)**, pp. 51-57.
11. Dorothy E. Denning. An Intrusion-Detection model. In *IEEE Symposium on Security and Privacy*, pages 118--131, 1986
12. Heberlein L.T, K. N. Levitt and B. Mukherjee. A method to detect intrusive activity in a networked environment. In *Proceedings of the 14th National Computer Security Conference*, pages 362-371, 1991
13. Heberlein, L., Dias, G., Levitt, K., Mukherjee, B., Wood, J., Wolber, D. A network security monitor. In *Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy*. pp. 296-304. 1990.
14. Herve´ Debar, Marc Dacier, Andreas Wespi. Towards a taxonomy of intrusion-detection systems. *Computer Networks 31 805–822.* 1999
15. http://www.deic.uab.es/material/26118-capitol1.pdf
16. https://www.owasp.org/index.php/Intrusion_Detection as at 5th may 2016
17. J Boudec and S Sarafijanovic. An artificial immune system approach to misbehavior detection in mobile ad-hoc networks. Technical Report IC/2003/59, Ecole Polytechnique Federale de Lausanne, 2003.
18. James Brentano, Stephen R. snapp, Gihan V. Dias, Terrance L. Goan, KarnlN. Levitt, Biswanath Mukherjee, Stephen E. Smaha: An architecture for a distributed intrusion detection system. Division of computer science, University of California Davis, California 95616.
19. James Brentano, Steven R. SnappGihan V. Dias, Terrance L.Goan, Karl N. Levitt, Biswanath Mukherjee, Stephen E. Smaha (1991) *"An architecture for a distributed intrusion detection system"* Division of Computer Science University of California 95616
20. K Begnum and M Burgess. A scaled, immunological approach to anomaly counter measures (combining ph with cfengine). *Integrated Network Management*, pages 31–42, 2003.
21. Karen Scarfone and Peter Mell. Guide to intrusion detection and prevention systems (IDPS). Technical Report SP800-94, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, U.S. Department of Commerce, July 2012.
22. Karen *Scarfone*. Peter *Mell*.(2012) Special Publication 800-94. Revision 1 (Draft) ... Natl. Inst. Stand. Technol. Spec. Publ. 800-94 Rev. 1, 111 pages (Jul. *2012*).
23. Marek Piotr Zielinski 2004: *Applying Mobile Agents In An Immune-System-Based Intrusion Detection System;* submitted in part fulfilment of the requirementsfor the degree of MASTER OF SCIENCE in the subject COMPUTER SCIENCE at theUniversity Of South Africa
24. Marek Piotr Zielinski. Applying mobile agents In an immune-system-based Intrusion detection system. *A dissertation submitted to the department of computer science, University of South Africa.* November 2004

25. Memon V. I. and ChandelG. S., (2014) "A Design and Implementation of New Hybrid System for Anomaly Intrusion Detection System to Improve Efficiency", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, vol. 4, Issue 5, (Version 1), May, pp. 01-07.
26. Mukherjee Biswanath, Todd L. Heberlein, and Karl N. Levitt, (1994) "*Network Intrusion Detection*", IEEE Network, May/June Creating a Complete Model of an Intrusion Detection System effective on the LAN.
27. Mukherjee Biswanath, Todd L. Heberlein, and Karl N. Levitt, (1994) "Network Intrusion Detection", IEEE Network, May/June
28. P. R. Subramanian and J. W. Robinson, (2012)"Alert over the attacks of data packet and detect the intruders", Computing, Electronics and Electrical Technologies (ICCEET), IEEE International Conference on ISBN: 978-1-4673-0211-1, **(2012)** March 21-22, pp. 1028-1031.
29. S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, C. Wee, R. Yip and D. Zerkle. Computer Security Research Group. The Design of GrIDS: A Graph-Based Intrusion Detection System. *Technical report*, UC Davis, Dept. of Computer Sc., May 14, 1997.
30. Sanjay Sharma and R. K. Gupta (2015) "*Intrusion Detection System: A Review."* International Journal of Security and Its Applications, *Vol. 9, No. 5 (2015), pp. 69-76 http://dx.doi.org/10.14257/ijsia.2015.9.5.07*
31. Stephanie Forrest, Alan S. Perelson, Lawrence Allen, and Rajesh Cherukuri. Self-nonself discrimination in a computer. In *Proceedings of the 1994 IEEE Symposium on Security and Privacy*, page 202. IEEE Computer Society, 1994.
32. Steven R. Snapp , James Brentano , Gihan V. Dias , Terrance L. Goan , L. Todd Heberlein , Che-lin Ho , Karl N. Levitt , Biswanath Mukherjee , Stephen E. Smaha , Tim Grance , Daniel M. Teal , Doug Mansur, DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and an Early Prototype, *In Proceedings of the 14th National Computer Security Conference* (1991)
33. Todd Heberline L, Gihan V. Dias, Karl N. Levitt, Biswanath Mukherjee, Jeff Wood, and David Wolber. (1990) A Network Security Monitor. In *IEEE Symposium on Research in Security and Privacy*, Pages 296--304, IEEE, May.
34. Uwe Aickelin, Julie Greensmith, and Jame Twycross (2004) "*Immune system approaches to intrusion detection- a review*" School of Computer Science University of Nottingham, UK.
35. WankhadeK., Patka S. and ThoolR., (2013) "An efficient approach for Intrusion Detection using data mining methods", International Conference on Advances in Computing, Communications and Informatics (ICACCI), Print ISBN:978-1-4799-2432-5 INSPEC Accession no. 13861274, August 22-25, pp. 1615-1618.
36. Yousef Farhaoui, Ahmed Asimi. (*2012)* "*Creating a Complete Model of an Intrusion Detection System effective on the LAN"*,International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 3, No. 5.