Volume 6, Issue 3, March 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review of Various Intrusion Detection Approaches

[1]Snehal V. Kale, [2]Surbhi R. Kale, [3]Rohini A. Naphade, [4]Prof. Abhay A. Dande.
[1, 2, 3] B.E. Final Year CSE Student, AEC Chikhli, Maharashtra, India
[4] Asst. Professor, CSE Department, AEC Chikhli, Maharashtra, India

Abstract-- Intrusion detection on the internet is a most interesting incomputer science today, where much work has been done in the last twodecades and still it has a great scope. To have sound understanding of the intrusion detection system concepts, the basic related terms need to be clearly understood. The paper here mainly briefs about the various methods available for intrusion detection.

Keywords*: *Intrusion, Threat, Vulnerability, Attack, Audit Records

I. INTRODUCTION

An intrusion is defined as any set of unauthorized actions that tries to create security threat to the integrity, confidentiality, or availability of resources of the system. An intrusion detection system (IDS) inspects all inside and outside network activities and identifies suspicious traffic patterns that may indicate a network or system attack from someone attempting to compromise a security system. An intrusion detection system attempts to detect these intrusions. In case of, network intrusion detection systems (NIDS), the primary source of data to be analyzed is network traffic while a host intrusion detection system (HIDS) depends on information collected on individual hosts.

II. APPROACHES TOINTRUSION DETECTION:

A. Misuse detection:

It is generally based on attack signatures and makes the use of rules, to detect intrusion. It is having high detection rate for those well-known intrusions, but many times not able to detect new intrusions. Misuse detection is based on the knowledge of system vulnerabilities and known attack signatures. It is able to find intruders who are attempting to break into a system by exploiting some known vulnerability. A large numbers of various types of rule sets can be used in misuse detection. Misuse detection systems use the rule set to look for events that possibly define an intrusion scenario. These rules can be If-then rules or even can be some model based rules.The events may be monitored live by monitoring system calls or later using audit records

B. Anomaly detection:

It defines the various patterns of normal behaviors. Any deviant from the normal profiles is considered asanomalies. It is quite difficult to exactly define the normal profile hence anomaly detection usually suffers from a higher false positive rate. Anomaly detection has assumption that an intrusion will always show some deviations from normally defined patterns.

Anomaly detection can be of static or dynamic anomaly detection. In static anomaly detection it is based on the assumption that there is a portion of the system being monitored that does not change. The static portion of a system is the code for the system and the constant portion of data upon which the correct functioning of the system depends. For example, the operating system software and data to bootstrap a computer never change. If the static portion of the system ever deviates from its original form, an error has occurred or an intruder has altered the static portion of the system.
Dynamic anomaly detection typically operates on audit records or on monitored networked traffic data. Audit records of operating systems do not record all events. They recordonly those events of possibly having intrusion.

C. Supervised and Unsupervised Learning Approach.

Now a days method from machine learning and pattern recognition are also used to detect intrusions. Supervised learning and unsupervised learning methods are used. Supervised learning methods for intrusion detection can only detect known intrusions. In supervised learning for intrusion detection, there are mainly supervised neural network (NN) based approaches and support vector machine based approaches are used.

Unsupervised learning methods can detect the intrusions that have not been previously learned. Examples of unsupervised learning for intrusion detection include *K*-means clustering based approaches and self-organizing feature map (SOM) based approaches.

.

D. Statistics-Based Approaches

Denning proposed a statistical method for intrusion detection. According to audit data, a profile is constructed to describe a given subject or a given object. Several metrics are defined for the profiles. The Gaussian models of the

metrics are constructed to detect intrusions. Vigna and Kemmerer use data that are sourced from network nodes, rather than the audit data, to construct profiles, enlightening the research on network-based intrusion detection. Some researchers propose more complex metrics and statistical models. Li and Manikopoulos propose some representative parameters of IP data flow, and they model the parameters using a hyperbolic distribution. In recent years, the hidden Markov model has been used in intrusion detection based on host auditdata.

III. CONCLUSION

In this paper we have discussed basic and important approaches for intrusion detection. Depending upon the requirement of the Intrusion Detection System and security constraints of the system any of the above mentioned approaches can be practically implemented. As a future scope of this paper, each of these approaches can be discussed in more detail with their various performance measurement parameters and comparative analysis.

REFERECES

[1] D. Denning, *"An intrusion detection model,"* IEEE Trans. Softw. Eng., vol. SE-13, no. 2, pp. 222–232, Feb. 1987.

[2] Z. W. Li, A. Das, and S. Nandi, *"Utilizing statistical characteristics of N-grams for intrusion detection,"* in Proc. Int. Conf. Cyberworlds, Dec. 2003, pp. 486–493.

[3] G. Vigna and R. A. Kemmerer, *"NetSTAT: A network-based intrusion detection approach,"* in Proc. Comput. Secur. Appl. Conf., Dec. 1998, pp. 25–34.

[4] J. Li and C. Manikopoulos, *"Novel statistical network model: The hyperbolic distribution,"* Proc. Inst. Electr. Eng.—Commun., vol. 151, no. 6, pp. 539–548, Dec. 2004.

[5] J. B. D. Caberera, B. Ravichandran, and R. K. Mehra, *"Statistical traffic modeling for network intrusion detection,"* in Proc. Model., Anal. Simul. Comput. Telecommun. Syst., 2000, pp. 466–473.

[6] William Stallings, Cryptography and Network Security: Principles and Practices, Pearson Education, 4th Edition, 2011.

[7] *"Understanding Intrusion Detection System"*, Internet, sans institute, 2001.

[8] Corinne Lawrence *"IPS – The Future of Intrusion Detection"* University of Auckland October 2004.

[9] Karthikeyan .K.R and A. Indra- *"Intrusion Detection Tools and Techniques a Survey"*

[10] Prof. S. Gore – *"Importance of Intrusion Detection System"*-International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011

