Intrusion Detection System

U. Tarun Rao#1, J. Sai Chand#2, S. Prithvi#3, Md. Salma#4

[1]B. Tech C.S.E TKREC Hyderabad Email: tarunraoutla@gmail.com
[2]B. Tech C.S.E TKREC Hyderabad Email: saichandgoud668@gmail.com
[3]B. Tech C.S.E TKREC Hyderabad Email: prithvi95.sp@gmail.com
[4]Asst.Professor, TKREC, Hyderabad, TS-India, Email: sajju.mohammad970@gmail.com

Abstract: Network Security is a primary concern in today's world of vast and complex networks. Rapid evolution of network technology has given way to several vulnerabilities in computer network infrastructures. The number of attacks trying to exploit these vulnerabilities is higher than ever, causing colossal damage to corporations and government organizations. This project aims to implement a Graphic user Interface based Intrusion detection system which parses weblogs for Virus Signatures stored over a database and helps network administrators identify compromised IP's over a large network.

Keywords: Network Security, Intrusion Detection System, Vulnerability Scanner.

I. Introduction

Computer networks are devoted infrastructures setup to facilitate the carrying of traffic such as data, voice, video etc. from one node to another. They consist of a varying number of nodes or stations, connected by various communication channels and devices. Large networks which need to be maintained by corporations or government organizations are built according to the client/ server network configuration model. In a client/server environment, a central high performance computer, the server, holds a majority of the files and other network resources. Other computers, known as 'clients', can access these resources. An advantage of a client/server network is that security is created, managed, and can be directly enforced. To access the network, a user must provide some credentials, such as a username and a password. If the credentials are not valid, the user is prevented from accessing the network.

Indicators of Compromise (IOC) are pieces of forensic data, such as data found in system log entries or files that identify potentially malicious activity on a system or network. Examples of IOC include unusual network traffic, unusual privileged user account activity, login anomalies, increases in database read volume, suspicious registry or system file changes, unusual DNS requests and Web traffic showing non-human behavior. These and other unusual activities allow security teams monitoring the systems and networks to spot malicious actors earlier in the intrusion detection process.

II. Existing & Proposed System

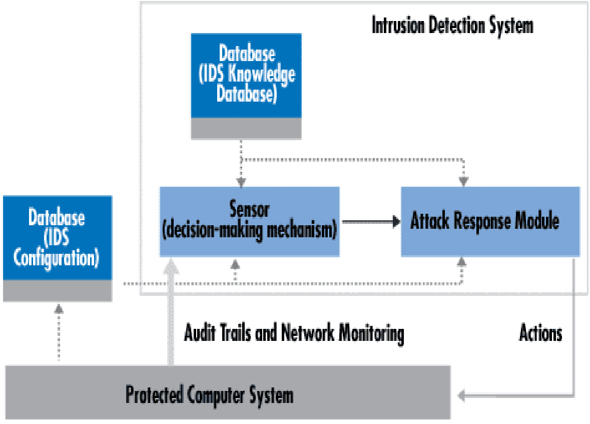
A. Existing System

Firewalls are not a cure-all solution to network security holes. Firewalls are only as good as the rule set. Anti-virus software uses virus definitions to identify threats However, virus definitions exist only for known attacks, new attacks can't be identified. In the current threat environment, rapid communication of pertinent threat information is the key to quickly detecting, responding and containing targeted attacks. Although security tools may not automatically recognize threats, they could help network administrators in doing so. A scanner needs to be created to parse weblogs and identify the compromised systems inside the network of NRSC (National Remote Sensing Centre), Hyderabad.

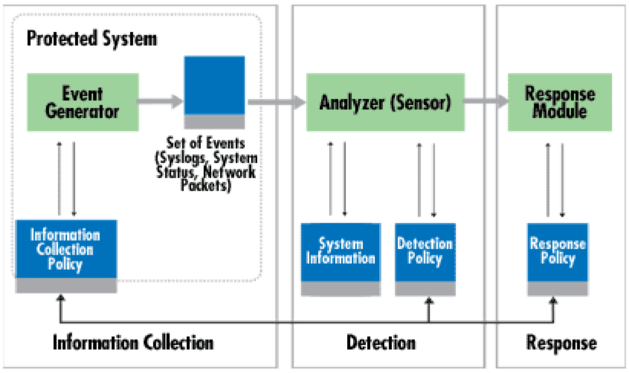
B. Proposed System

IOC Bucket is a global community of computer security professionals who have a vested interest in sharing Indicators of Compromise (IOC) discovered during their research. IT departments are often overwhelmed by an ever-increasing flood of Indicators of Compromise (IOC) detailing illicit activity that may occur on their networks and systems. The characterization of the threats involved varies with the source of the information and each notice requires human operators to shift through data as displayed on a web page or in a PDF, update monitoring appliances and if detected, decide on appropriate remediation. Through the contributions of industry standard OpenIOC's, IOC Bucket is the largest repository of Open Source Indicators which stores threat information in a standard format. IOCs include IP addresses, domains, file hashes, URLs, CVE numbers etc, which can be used to identify the presence of malicious content. A GUI based vulnerability scanner could be developed using open source IOCs to scan a weblog and notify the network administrator of the systems that could be compromised.To save scan time and improve efficiency, attack specific databases can be defined and used.

III. System Architecture


Intrusion Detection System
Database (IDS Knowledge Database)
Database (IDS Configuration)
Sensor (decision-making mechanism)
Attack Response Module
Audit Trails and Network Monitoring
Actions
Protected Computer System

Sensors are placed in the network to monitor activities and network behavior is analyzed with the knowledge of normal, abnormal and malicious activities. Based on analysis, network administrators are notified about threats and attacks.



Logs are used to collect information about network activities, which are analyzed. Attacks are detected based on the rule set. Then, appropriate response is taken to prevent or mitigate attacks.

IV. Algorithm

Signature-Based Detection, Signature based IDS monitor’s packets in the Network and compares with pre-configured and pre-determined attack patterns known as signatures.

Statistical anomaly-based detection, An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network – what sort of bandwidth is generally used and what protocols are used. It may however, raise a False Positive alarm for legitimate use of bandwidth if the baselines are not intelligently configured.

Stateful Protocol Analysis Detection, This method identifies deviations of protocol states by comparing observed events with “predetermined profiles of generally accepted definitions of benign activity.

V. Modules

User Module

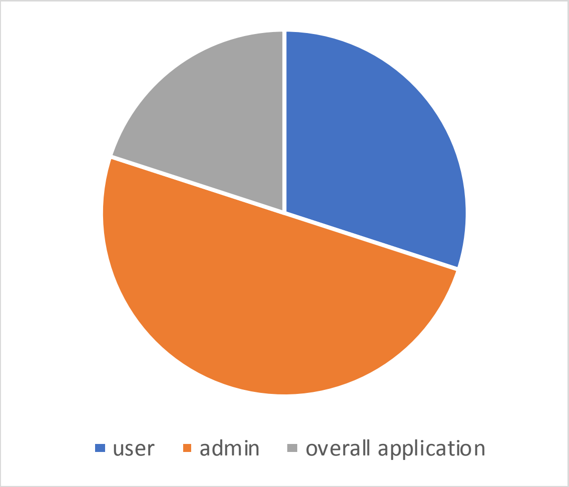
Loads the network LOG file to be scanned. Compares the Log file to the database for any virus signatures to find out compromised IP's over the network.

Admin Module

Ads the virus signatures into the database from the IOC (Indicators of compromise) file and modifies the database as required.

VI. Result Analysis

The majority of the functionalities are available to the Administrator so 50% is assigned. User module when compared to Overall application has more functionality so 30% is assigned.



VII. Conclusion

This paper presents an overview of the development and implementation of Intrusion Detection System as a Server Side application. The results obtained from implementation are encouraging and promising for development of more complex systems in the future. The vulnerability scanner which has been developed cannot completely eliminate attacks, however, it can ease the burden of network administrators by filtering data to a large extent. As sophistication of attacks is increasing at an alarming rate, analysis of networks by humans will be a tedious task.

VIII. Future Enhancements

In proposed Intrusion Detection System there is scope for improvement, detection mechanisms, artificial neural networks can be used to update attack signatures in real time and intelligently monitor and classify network activities to be abnormal or suspicious.

IX. References

[1] Abdullah A. Mohamed, "Design Intrusion Detection System Based On Image Block Matching", International Journal of Computer and Communication Engineering, IACSIT Press, Vol. 2, No. 5, September 2013.

[2] "Gartner report: Market Guide for User and Entity Behavior Analytics". September 2015.

[3] "Gartner: Hype Cycle for Infrastructure Protection, 2016".

[4] "Gartner: Defining Intrusion Detection and Prevention Systems". Retrieved September 20, 2016.

[5] Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)" (PDF). Computer Security Resource Center. National Institute of Standards and Technology (800–94). Retrieved 1 January 2010.

[6] "NIST – Guide to Intrusion Detection and Prevention Systems (IDPS)" (PDF). February 2007. Retrieved 2010-06-25.

[7] Robert C. Newman (19 February 2009). Computer Security: Protecting Digital Resources. Jones & Bartlett Learning. ISBN 978-0-7637-5994-0. Retrieved 25 June 2010.

[8] Michael E. Whitman; Herbert J. Mattord (2009). Principles of Information Security. Cengage Learning EMEA. ISBN 978-1-4239-0177-8. Retrieved 25 June 2010.

[9] Tim Boyles (2010). CCNA Security Study Guide: Exam 640-553. John Wiley and Sons. p. 249. ISBN 978-0-470-52767-2. Retrieved 29 June 2010.Engin Kirda; Somesh Jha; Davide Balzarotti (2009). Recent Advances in Intrusion Detection: 12th International Symposium, RAID 2009, Saint-Malo, France, September 23–25, 2009, Proceedings. Springer. p. 162. ISBN 978-3-642-04341-3. Retrieved 29 June 2010.

[10] Grace, Clive. "Understanding intrusion detection systems."*PC Network Advisor* 122 (2000): 11-15.

[11] Akbar, Shaik, K. NageswaraRao, and J. A. Chandulal. "Intrusion detection system methodologies based on data analysis." International Journal of Computer Applications 5, no. 2 (2010): 0975-8887.

[12] Rao, AllamAppa, P. Srinivas, B. Chakravarthy, K. Marx, and P. Kiran. "A Java Based Network Intrusion Detection System (IDS)." In Proceedings of The, pp. 206-118. 2006.

[13] Rhoades, Doug. "Machine actionable indicators of compromise."In Security Technology (ICCST), 2014 International Carnahan Conference on, pp. 1-5.IEEE, 2014.

[14] Daya, Bhavya. "Network security: History, importance, and future "University of Florida, Department of Electrical and Computer Engineering(2013).