RESEARCH PAPER | Information Technology | Volume : 2 | Issue : 3 | December 2012 | ISSN - 2249-555X

Open Source Intelligent Network Intrusion Detection System Analyzer

KEYWORDS: Anomaly, Attacks, Detection, IDS, Information Security, Intruders, Signature.

Bhavini Ahir	Prachi Tambakhe	Dr. Kalpesh Lad
Uka Tarsadia University, Bardoli, Surat - 394 350 Gujarat (INDIA)	Uka Tarsadia University, Bardoli, Surat - 394 350 Gujarat (INDIA)	Uka Tarsadia University, Bardoli, Surat - 394 350 Gujarat (INDIA)

ABSTRACT *Today computers are part of networked; distributed systems that may span multiple buildings sometimes located thousands of miles apart. The network of such a system is a pathway for communication between the computers in the distributed system. The network is also a pathway for intrusion. Intrusion detection is an important technology in business sector as well as an active area of research. It is an important tool for information security. A Network Intrusion Detection System is used to monitor networks for attacks or intrusions and report these intrusions to the administrator in order to take evasive action. This system is designed to detect and combat some common attacks on network systems. It follows the signature based IDs methodology for ascertaining attacks. A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. In this system the attack log displays the list of attacks to the administrator for evasive action. This system works as an alert device in the event of attacks directed towards an entire network. This paper discuss about various architecture of network intrusion detection system & their limitations and advantages. Snort is used as NIDS & its output is used by Open Source Intelligent Network Intrusion Detection System Analyzer for generating various reports for analysis.*

1. INTRODUCTION

Due to the rapid growth in the technology and widespread use of the Internet, a lot of problems have been faced to secure the system's critical information within or across the networks because there are millions of people attempting to attack on systems to extract confidential and critical information. A huge number of attacks have been observed in the last few years. Only the smooth network connectivity can ensure that clients will use it for online shopping, communication, debit and credit card details and exchange of personal information etc.

Security is an important and serious issue for every type of network. Many network environments specially those where computers are used as nodes are prone to an increasing number of security threats in the form of Trojan worm attacks and viruses that can damage the computer systems, servers and communication channels [1]. Though Firewalls are used as a necessary security measure in a network environment but still different types of security issues keep on arising. In order to further strengthen the network from intruders, the concept of intrusion detection system (IDS) and intrusion prevention system (IPS) is gaining popularity [1],[2].

The majority of network communications occur in an unsecured format, which allows an attacker to access and read traffic of network. There are various ways to attack into networks such as IP address spoofing attack, Password-based attack, Man-in-the-Middle Attack and Sniffer Attack [15].The purpose of network security is essentially to prevent loss, through misuse of data. There are a number of potential pitfalls that may arise if network security is not implemented properly such as breaches of confidentiality, data destruction, and data manipulation [3]. A Network Intrusion Detection System is used to monitor networks for attacks or intrusions and report these intrusions to the administrator in order to take evasive action [1].

2. INTRUSION DETECTION SYSTEM

Intrusion detection is a type of security management system for computers and networks. An ID system gathers and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions and misuse. ID uses vulnerability assessment, which is a technology developed to assess the security of a computer system or network [6].

Intrusion detection is the art and science of sensing when a network is being used inappropriately or without authorization. An intrusion-detection system (IDS) monitors system and network resources and activities and, using information gathered from these sources, notifies the authorities when it identifies a possible intrusion [7]. It inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. In general, the techniques for intrusion detection fall into two major categories depending on the modelling methods used: misuse detection and anomaly detection [1].

- Misuse detection compares the usage patterns for knowing the techniques of compromising computer security. Although misuse detection is effective against known intrusion types; it cannot detect new attacks that were not predefined. Anomaly detection, on the other hand, approaches the problem by attempting to find deviations from the established patterns of usage [1].
- Anomaly detection may be able to detect new attacks. However, it may also cause a significant number of false alarms because the normal behaviour varies widely and obtaining complete description of normal behaviour is often difficult. Architecturally, an intrusion detection system can be categorized into three types host based IDS, network based IDS and hybrid IDS [1].

IDSs based on various parameters. The Standard models are Rule-based Detections and Statistical Anomaly Detection [5]. Statistical anomaly detection systems are grouped into Profile based detections and threshold detection. There are Network based [8],[12], Host based [1],[8],[12] and Stego [5] type intrusion detection system. A host based intrusion detection system uses the audit trails of the operation system as a primary data source [1],[8]. A network based intrusion detection system, on the other hand, uses network traffic information as its main data source [8]. A stego based intrusion detection uses steganalysis to discover any occurrence of stego content in data or media to prevent stego intrusions [5]. The main problem is the difficulty of distinguishing between natural behaviour and abnormal behaviour in computer networks due to the significant overlap in monitoring data. This detection process generates false alarms resulting from the Intrusion Detection based on the anomaly Intrusion Detection System [4]. There is two different ways to study the

Volume : 2 | Issue : 3 | December 2012 | ISSN - 2249-555X

false positive reduction either study the false alert reductions at the sensor level or at the log alert file [9].

3. DEVELOPMENT APPROACHES IN NETWORK BASED INTRUSION DETECTION SYSTEM

Network based intrusion detection systems attempts to identify unauthorized, illicit, and anomalous behaviour based solely on network traffic. A network IDS, using either a network tap, span port, or hub collects packets that traverse a given network. Using the captured data, the IDS system processes and flags any suspicious traffic. It does not actively block network traffic. The role of a network IDS is passive, only gathering, identifying, logging and alerting [4], [10],[11],[13],[14]. Following are various approaches to provide NIDS:

3.1Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection

The problem of false positives in intrusion detection by building an alert classifier that tells true from false positives. Alert classification is defined as attaching a label from a fixed set of user-defined labels to an alert. In the simplest case, alerts are classified into false and true positives, but the classification can be extended to indicate the category of an attack, the causes of a false positive or anything else [10]. Alert classifiers can be built automatically using machine learning techniques or they can be built manually by human experts.

ALAC is alert classifiers whose classification logic is explicit so that a human expert can inspect it and verify its correctness. In that way, the analyst can gain confidence in ALAC by understanding how it works [10]. In this system, analysts do not write alert classification rules themselves or do not write them more frequently. Analyst might be able to individually classify some alerts as false positives, but may not be able to write a general rule that characterizes the whole set of these alerts and classification of alerts may also change. As a result, rules maintenances and management process is labour-intensive and error-prone for ALAC [10]. This system is useful in agent mode, where some alerts are autonomously processed. It evaluates the performance of the system on the basis of more realistic intrusion detection data and to integrate an alert correlation system to reduce redundancy in alerts [10].

3.2ATLANTIDES: An Architecture for Alert Verification in Network Intrusion Detection Systems

It is alert verify in network intrusion-detection systems. It is based on a systematic anomaly based analysis of the system output, which provides useful context information regarding the network services. The false positives raised by the NIDS analysing the incoming traffic are reduced by correlating them with the output anomalies [11]. False alerts also cause an overload for IT personnel, who must verify every single alert, a task that is not only labour intensive but also error prone [11].

ATLANTIDES is an innovative architecture for easing the management of any NIDS by reducing, in an automatic way, the number of false alarms that the NIDS raises [11]. It cannot work properly with encrypted data unless the cryptographic keys are provided. It works in combination of signature-based and anomaly-based NIDSs and no need of human involvement in NIDS management [11].

3.3Novel Approach to IDS using Data Mining & Mobile Agent

The mobile agent is an agent having the capability of moving from one host to another. The advantages of mobile agent technology includes: reducing network overload, overcoming network latency, synchronous and autonomous execution, robustness and fault-tolerance, system scalability, and operating in heterogeneous environments [13]. To this end, mobile agent technology has been shown to be very suitable to solve intrusion detection in a distributed environment [13].

The MAD-IDS system integrates the data mining algorithms and a mobile agent technology in a network intrusion detection to detect both known and novel attacks [13]. Main objective is to detect known and unknown attacks with a high accuracy in a distributed environment and reduce false alarms. MAD-IDS are feasible for detecting attacks within a distributed environment [13].

3.4Game Theory and Intrusion Detection System

The game theory utilized in intrusion detection systems for assisting in defining and reconfiguring security policies given the severity of attacks dynamically. Furthermore, a game theoretic approach to intrusion detection systems assist in the decision process involved with allocation or reallocating limited resources for detecting significant threats to vital subsystems of a large networked system in near real time [14]. The aim of a game theoretic approach to intrusion detection systems should allow for the quantification of appropriate responses that would match threat levels.

Although the introduction of game theory into the realm of network-based intrusion detection systems presents a vast improvement over existing methods, there is no perfect solution as of yet [14]. The weakness of the game theoretic approach to intrusion detection is the unsolved approach on how to detect and handle simultaneous attacks [14].

3.5Design Network Intrusion Detection System using Hybrid Fuzzy-Neural Network

This model takes advantage of different classification abilities of fuzzy logic and neural network for intrusion detection system. It has ability to recognize an attack, to differentiate one attack from another, classifying attack, and the most important, to detect new attacks with high detection rate and low false negative [4].

Neural Networks were specifically proposed to learn the typical characteristics of system's users and identify statistically significant variations from their established behaviour [4]. Neural Network based models on simultaneously explorer several hypotheses make the use of several computational interconnected elements; this parallel processing may imply time savings in malicious traffic analysis [4].

3.6A Unified Approach for Real Time Intrusion Detection using Intelligent Data Mining Techniques

This approach uses the combined strategies of Data Mining and Expert Systems were used to design IDS. Data Mining makes use of algorithms to extract useful information, patterns and trends often previously unknown. The challenge in using these techniques is to detect and/or prevent attacks and eliminate False Positives and False Negatives as much as possible [16]. Neural Networks is used it is clear that the learning speed of the network is generally slower and a research challenge is to improve performance of learning algorithm [16].

The SLFN algorithm is used and applied to the decision tree to improve the performance of the learning rate and the new attacks found are updated to the training set accordingly for further processing [16]. Designing the IDS for a real time has become even more challenging. Real time learning capability of Neural Networks is the need whenever a new threat is faced, where a new knowledge map has to be built [16].

3.7Application of Artificial Intelligence in Network Intrusion Detection-A Succinct Review

This approach is useful not only in detecting successful intrusions, but also in monitoring attempts to break security, which provides important information for timely counter-measures. An Artificial Intelligence (AI) technique has been employed in different data mining and machine learning classification and prediction modelling schemes [17]. AI naturally transformed into Computational Intelligence (CI) with the introduction of the concept of Machine Learning.

A major focus of machine learning research is to automatically learn to recognize complex attributes and to make intelligent decisions based on the correlations among the data

Volume : 2 | Issue : 3 | December 2012 | ISSN - 2249-555X

variables [17]. The hybrid learning combines the supervised and unsupervised techniques to generate an appropriate function and to meet a specific need of solving a problem. The computational analysis of machine learning algorithms and their performance is a branch of theoretical computer science known as computational learning theory. The ensemble and hybridization of various Artificial Intelligence techniques also indicate a bright future in the analysis of IDS and the prediction of its various properties for effective real-time network security [17].

4. OPEN SOURCE INTELLIGENT NETWORK INTRUSION DETECTION SYSTEM ANALYZER

Authors proposed an approach for analyzing the log file created as output of the Snort open source software. Snort is an open source network intrusion prevention and detection system. It uses a rule-based language combining signature, protocol and anomaly inspection methods to help analyst. It is most widely deployed intrusion detection and prevention technology and it has become the de facto standard technology worldwide in the industry.

A packet sniffer will capture and display packets from the network with different levels of detail on the console. Packet logger will log data in text file. Honey pot monitor will deceiving hostile parties. Packet Decoder takes packets from different types of network interfaces (Ethernet, SLIP, PPP…), prepare packets for processing.

Pre-processor will (1) prepare data for detection engine; (2) detect anomalies in packet headers; (3) packet defragmentation; (4) decode HTTP URI; (5) reassemble TCP streams. Detection Engine the most important part, applies rules to packets. Logging and Alerting System will generate the alerts and logs file. Output Modules process alerts and logs and generate final output.

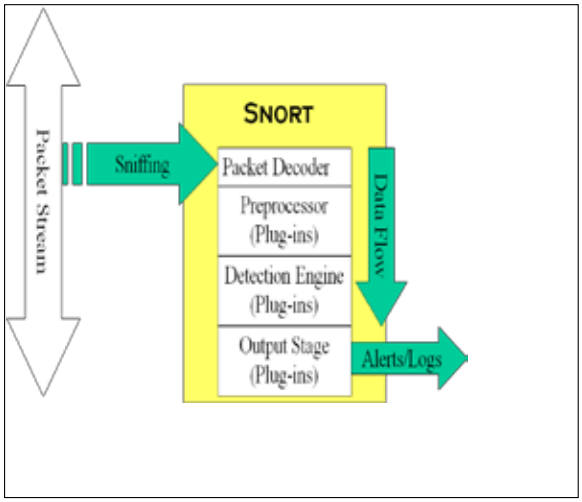

Figure 1: Snort Architecture

A tool for analyzing the snort output which are as log files. This tool will provide user interface for analyzing the alerts & generate various reports with different perspective as per the need. It also generate automated database as per the log file / alerts' format. Each entry of log file & alert is appended in the database daily.

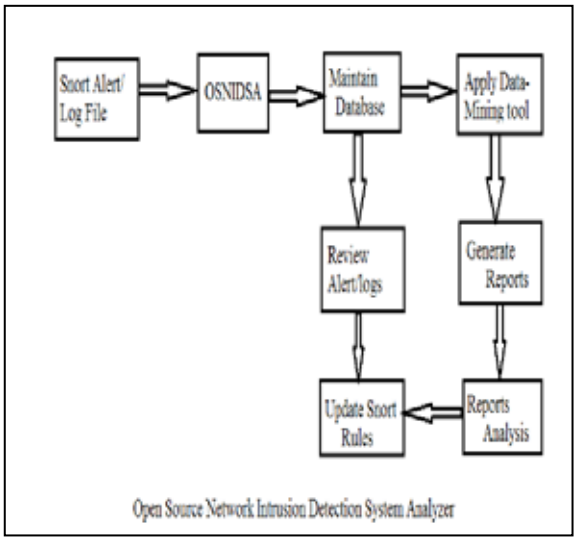

Figure 2: Open Source Intelligent Network Intrusion Detection System Architecture

The data mining tools can be apply on database to generate reports with different data perspective & also used to find unknown pattern from the large data repository. This can help to take wise decision while reviewing the output of SNORT/ Log file. Weka & Rapid Miner is Java based open source data mining tool.

The proposed Analyzer will perform various queries on the database as per the need. It can also review the alerts and log. It provides labelling to the logs & alerts for future signature detection and help analyst to update the snort rules.

5. CONCLUSION

In this paper, authors have discussed about various architectures of Network Intrusion detection system & its limitation. Our aim is to evaluate the performance of the system on the basis of more realistic intrusion detection data and to integrate an alert correlation system to reduce redundancy in alerts. One possible extension to these architectures is adding additional information to make the detection of anomalies in the output more precise. While going through various architectures, it is true that the systems require more human efforts for analyzing, verifying & correcting the log file. So Snort Analysis Software is used to make database of snort output & perform various queries to generate reports. These reports can be used by analyst to analyze the network traffic, true positive & false positive attack and update the snort rule.

Volume : 2 | Issue : 3 | December 2012 | ISSN - 2249-555X

REFERENCE

1. Usman Asghar Sandhu, Sajjad Haider, Salman Naseer, and Obaid Ullah Ateeb, "A Study of the Novel Approaches Used in Intrusion Detection and Prevention Systems", International Journal of Information and Education Technology, Vol.- 1, No-. 5, December 2011 | 2. Lei WEI, "Evaluation of Intrusion Detection Systems",lwei026 4526704, 23 October 2007 | 3. Karishma Sundaram , "Why is Network Security Important?", Article on www.brighthub.com, last updated on 4/22/2010 | 4. Muna Mhammad T. Jawhar & Monica Mehrotra, "Design Network Intrusion Detection System using hybrid Fuzzy-Neural Network", International Journal of Computer Science and Security, Volume -4, Issue-3 PP 293 | 5. Ganta Jacob Víctor, Sreenivasa Rao Meda, V CH Venkaiah, "False Positives in Intrusion Detection Systems" | 6. Margaret Rouse,"Intrusion Detection (ID)", Article on www.searchmidmarketsecurity.techtarget.com, last updated May 2007. | 7. Ravneet Kaur, "Advances in Intrusion Detection System for WLAN", Advances in Internet of Things, 2011, 1, 51-54, Published Online October 2011 | 8. Homam El-Taj, Omar Abouabdalla, Ahmed Manasrah, "FALSE POSITIVE REDUCTION IN INTRUSION DETECTION SYSTEM: A SURVEY", Proceedings of IC-BNMT in 2009 | 9. Tadeusz Pietraszek, "Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection", Article on www.citeseerx.ist.psu.edu , last updated :2004 | 10. Damiano Bolzoni,Bruno Crispo,Sandro Etalle, "ATLANTIDES: An Architecture for Alert Verification in Network Intrusion Detection Systems", 21st Large Installation System Administration Conference (LISA '07) | 11. Hakan Albag, "Network & Agent Based Intrusion Detection Systems", Article on www.model.in.tum.de, last updated 7th June 2012 | 12. Imen Brahmi, Sadok Ben Yahia, and Pascal Poncelet, "MAD-IDS: Novel Intrusion Detection System using Mobile Agents and Data Mining Approaches", Article on www.citeseerx.ist.psu.edu, last updated 6th July 2012 | 13. Anis Alazzawe, Asad Nawaz and Murad Mehmet Bayraktar, "Game Theory and Intrusion Detection System", ISA 767-SecureE-Commerce Spring 2006 | 14. Article available on www.technet.microsoft.com , last updated on 8th August 2012. | 15. Naveen N C,Dr. R. Srinivasan,Dr. S. Natarajan, "A Unified Approach for Real Time Intrusion Detection using Intelligent Data Mining Techniques", IJCA Special Issue on "Network Security and Cryptography" NSC, 2011 | 16. Fatai Adesina Anifowose,Safiriyu Ibiyemi Eludiora, "Application of Artificial Intelligence in Network Intrusion Detection A Succinct Review", World Applied Programming, Vol-2, No-3, March 2012. PP 158-166 ISSN: 2222-2510 www.waprogramming.com.