Journal of Engineering Sciences
Vol 11, Issue 4 , April/2020
ISSN NO:0377-9254

A DETAILED STUDY ON ANAMOLY BASED INTRUSION DETECTION SYSTEM

Dr. Varanasi Usha Bala[1], M. J.Sarika[2], G.prudhvi[3], K.Sharmila[4],
M. Sri Mounica[5]
[12345] Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam
{ushabala.cse@anits.edu.in}
{sarikamanepalli321, srimouni1999} @gmail.com

Abstract- *Attacks on the internet keep on increasing and it causes harm to our security system. In order to minimize these threats and attacks, it is necessary to have a security system that has the ability to detect these attacks and analyze them. This is where an intrusion detection system comes into the picture. Intrusion detection is the process of identifying and responding to suspicious activities targeted at computing and communication resources, and it has become the mainstream of information assurance as there is a dramatic increase in the number of attacks. Intrusion detection system (IDS) monitors and collects data from a target system that should be protected, processes and correlates the gathered information, and initiates responses when evidence of an intrusion is detected. We need to suggest a proactive technique that helps to monitor and take necessary action depending upon the behavior of the network. Our main goal is to detect a method to protect our data from malicious activity.*

Keywords: *Intrusion, Intrusion Detection System, Attack, Wormhole Attack, Blackhole Attack.*

1. INTRODUCTION

Intrusion Detection System, Network-based Intrusion Detection System and Hybrid Intrusion Detection System. Network-based intrusion detection system collects input file by monitoring network traffic. Host-based intrusion detection system collects input file from the host it monitors. Hybrid intrusion detection system collects input file from both of network traffic and hosts it monitors. There are two techniques Anomaly Detection and Misuse Detection Anomaly detection refers to intrusions which will be detected supported anomalous behavior and use of computer resources. Anomaly detection usually uses methods of statistical analysis methodology, artificial neural network technology, data processing technology, and artificial immune technology. Misuse intrusion detection refers to the detection of intrusions by precisely defining them before time and expecting their occurrences. Misuse intrusion detection usually use methods of expert system, TCP/IP protocol analysis, and pattern matching. During this paper, we designed and implemented a host-based intrusion detection system, which uses pattern matching and BP neural network as its detection methods. Firstly, the log files are used as its primary sources of data in HIDS, and thru three steps of pre-decoding log file, decoding log file, and analysis log file, it can effectively identify various intrusions. Secondly, supported Black hole attack and wormhole attack and establishment of system behavior characteristics profile beforehand, the HIDS can identify intrusions by comparison with threshold. These results show that the HIDS can effectively improve the efficiency and accuracy of intrusion detection[2].

Any malicious activities present during a system or during a network are often detected by an Intrusion Detection System[1].Set of rules are defined to stop the intrusion with the assistance of IDS.
These set of rules generates alert messages or signals while detecting the intrusion during a system or a network. IDS is especially classified into Host-Based Intrusion Detection System Network Intrusion Detection System supported the sort of the systems the IDS protects. Signature Based Intrusion Detection System, Anomaly Based Intrusion Detection System are classified supported the tactic of working. HIDS analyses the incoming and outgoing packets from a system. This also monitors the OS of the pc. NIDS monitors traffic on a private network by continuously performing traffic analysis then comparing it with detected or known attacks within the library. However IDS monitors mischievous activities, they could also generate False Alarms. Therefore the speed of False Alarms should be less when IDS is implemented[3].
The rest of the paper is organized as follows. Section

II contains related work of NS2,OSSEC,SNORT, Section III contains the methodology of the work being done, Section IV contains how the work is implemented , Section V contains all the obtained results, Section VI concludes the paper along with a proposal of future scope.

2 . RELATED WORK

Existing tools for intrusion detection system:
NS2, OSSEC, SNORT

2.1 NS2

The intrusion detection is evaluated by simulation in presence of nodes that can take different attacks. It is capable of detecting a false information attack using statically techniques and can also detect other types of attacks. Many intrusion detection systems have been proposed and most of them are routing protocols like route guard etc. It resides in each node and is based on overhearing. Through overhearing each node can detect the malicious action of its report and other nodes. If the node is overhearing itself then it is malicious and then it cause serious impact on network performance. Its ability to discover the malicious nodes which can partition the network by falsely reporting the nodes and proceed to protect the network.

2.2 OSSEC

It is one among the simplest open source application.[4] It's an incredibly efficient processor, but it doesn't have a use interface when it involves log data. It organizes your log files and use anomaly based intrusion detection and it offers log file detection methods and scan for unauthorized changes could specifically cause issue.

2.3 SNORT

It is an open source NIDS application. It also used in packet sniffing and logging functionality. It allows predefined rules for snort are available on the website. The rule set includes both anomaly and signature based detection systems.

3 METHODOLOGY

3.1 Log Monitor

It has map and visualize devices dependency to optimize the bandwidth and traffic.

3.2 Connector

Networks connect computers and therefore the users of these computers. Individuals within a building or work group are often connected into LAN. Trace file that was generated by ns, or we will execute it directly out of the TCL simulation script for the simulation which we would like to see. Below we will see a screenshot of a NAM window where the foremost important functions are being explained.

3.3 Log analysis

It is the process of monitoring the events occurring in a computer or network and analyzing[5] them for signs and imminent threats of the security.

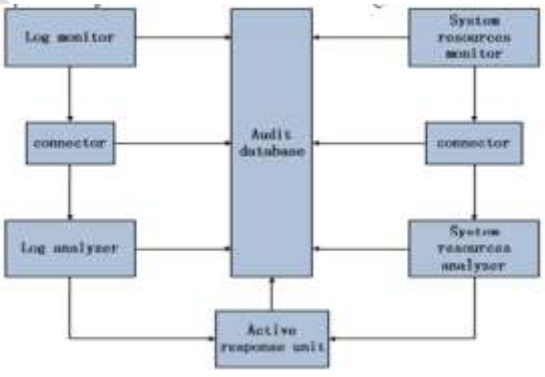

Fig 1 System Architecture

3.4 Audit Database

inserted with a script and it can be configured to scan your network and device immediately.

3.5 Active response unit

The intrusion detection monitors for attacks and provides information services and IDS actively stops the threat. It can be configured to scan your network and devices automatically.

4. IMPLEMENTATION

NS2 is a distinct event simulator focused on networking research. NS2 imparts considerable support for simulation of routing protocols over wired and wireless networks. In users perspective, NS2 is an Octal interpreter that takes an Octal script as input and produces a trace file as output. There are two sets of languages in NS2 (C++ and Octal) . C++ is utilized for creation of objects to maintain speed and efficiency. Octal is utilized as a front-end to setup the simulator and to configure the objects. The common procedure for generating a simulation can be classified into various steps.

They are:

- •Topology definition
- •Node and link configuration
- •Execution
- •Performance analysis
- •Graphical Visualization (X graphs)

A mobile ad-hoc network (MANET) is a kind of wireless ad-hoc network, and is a self-configuring network of mobile routers (and associated hosts) connected by wireless links – the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology[7]may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet.

5 RESULT

This presents the stimulation result of the proposed system with the help of NS2

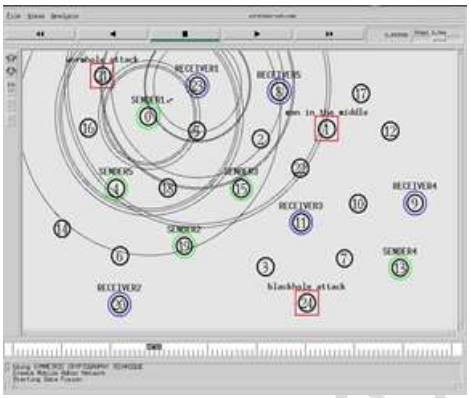

Fig 2. Creating Mobile Adhoc Network

This figure shows an Adhoc network created. The rest of the figures show comparison of different factors like packet overhead, through put, delay and PDR of the proposed system with the existing system

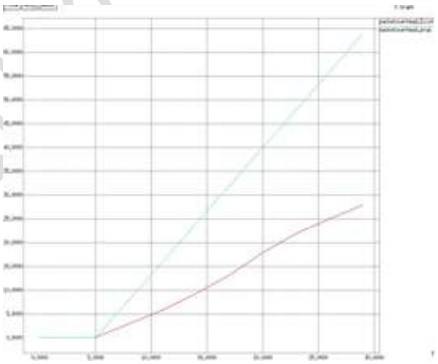

Fig 3. Comparison of packet over head of the proposed with the existing system.

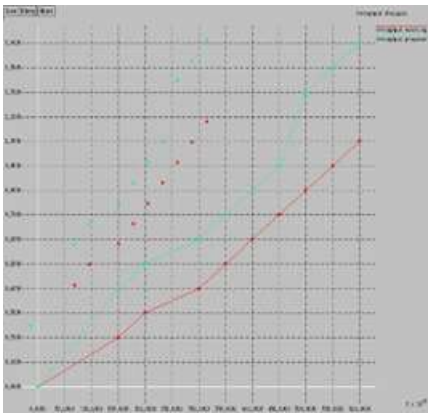

Fig 4: Comparison of throughput of the proposed with the existing system

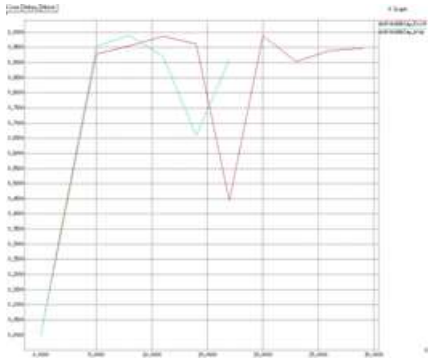

Fig 5. Comparison of end delay of the proposed with the existing system.

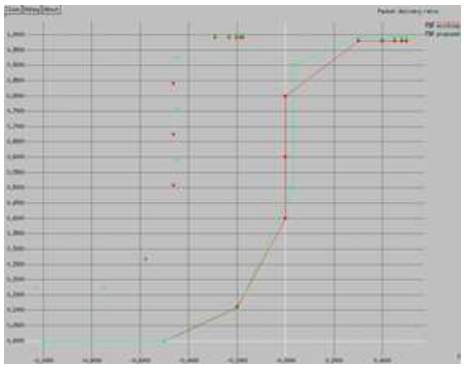

Fig 6. Comparison of PDR of the proposed with the existing system

6 . CONCLUSION AND FUTURE WORK

To the best of the authors' knowledge, this paper demonstrates, for the first time, that it is possible to create simple and effective shortest path[6] distribution in scale-free network topologies by accounting for the number of nodes only. The accuracy of the proposed models has been further investigated by considering real Internet network topologies, learned from reference data sets. This work represents a strong advancement of the state of the art because currently available approaches require a case-by-case fitting to catch the properties of the network scenario of interest. For future works, we plan to apply this approach to other distributions, such as Weibull, in order to achieve even better accuracy.

ACKNOWLEDGEMENT

We thank Prudhvi for his enormous assistance in evaluating our system and supporting us throughout the analysis.

REFERENCES.

[1] Dorothy Denning, "An Intrusion Detection Model", IEEE Transactions on Software Engineering, February 1987, pp.2- 222.
[2] G. Vigna and C. Krueger, "Host-based Intrusion Detection Systems, " in The Handbook of Information Security, Volume III, John Wiley &Sons, December 2005.
[3] Sandeep Kumar, Eugene H. Spafford, "An application of Pattern Matching in Intrusion Detection", Technical report 94-013,PurdueUniversity, Department of computer sciences, March 1994.
[4] Daniel B. Cid, OSSEC[OL] , 2008.
[5] Andrew Hay, Daniel Cid, Rory Bray, Log Analysis using OSSEC[M],Synereses, 2007.
.[6] Yen, J.C. and J.I. Guo, 2002, "The design and realization of a chaotic neural signal security system", Pattern Recognition and Image Analysis (Advances in Mathematical Theory and Applications), 12,pp.70-79.
[7] Lian, S., G. Chen, A. Cheung and Z. Wang, 2004. A chaotic-neural network-based encryption algorithm for JPEG2000 encoded images Advances in Neural Networks, Intl. Syme. Neural Networks., Part II, Lecture Notes in Computer Science, 3174,pp.627-632.