ABSTRACT

Attacks on the internet keep on increasing and it causes harm to our security system. In order to minimize these threats, 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 system (IDS) monitors and collects data from a target system that should be protected, processes and correlates the gathered 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.

TABLE OF CONTENTS

LIST OF FIGURES

1.INTRODUCTION

1.1 INTRODUCTION

An 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. Depending on their source of input, IDSs can be classified into Host-based Intrusion Detection System (HIDS), Network-based Intrusion Detection System (NIDS) and Hybrid Intrusion Detection System. Network-based intrusion detection system collects input data by monitoring network traffic. Host-based intrusion detection system collects input data from the host it monitors. Hybrid Intrusion detection system collects input data from both of network traffic and hosts its monitors. “Anomaly” detection and “Misuse” detection are two main techniques that HIDS use. Anomaly detection refers to intrusions that can be detected based on anomalous behaviour and use of computer resources. Anomaly detection usually uses methods of statistical analysis methodology, artificial neural network technology, data mining technology, an artificial immune technology. Misuse intrusion detection refers to the detection of intrusions by precisely defining them ahead of time and watching for their occurrences. Misuse intrusion detection usually use methods of expert system, TCP/IP protocol analysis, and pattern matching. In 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 HIDS uses log files as its primary sources of information, and through three steps of pre-decoding log file, decoding log file, and analysis log file, it can effectively identify various intrusions. Secondly, based on BP neural network analysis technology and through establishment of system behaviour characteristics profile in advance, the HIDS can identify intrusions by comparison with threshold. Experiment results show that the HIDS can effectively improve the efficiency and accuracy of intrusion detection.

In an increasingly interconnected environment, information is exposed to a wide variety of risks. So we have to provide security to the information. Information security is not all about securing information from unauthorized access, it is basically the practice of preventing unauthorized access, use, disclosure, modification. Implementing, maintaining and updating information security in an organization becomes a challenge. We need

information security to reduce the risk to a level that is acceptable to the business. The proposed system mainly protects the information from unauthorized access. It protects the information from modification and destruction. The objectives of Information Security are CIA (confidentiality, integrity, availability). Information that is provided can be in any form. Information from social media, data on your laptops or computers, etc. are examples of information security.

Any malicious activity present in a system or in a network can be detected by an Intrusion Detection System. Set of rules are defined to prevent the intrusion with the help of IDS.

This set of rules generates alert messages or signals while detecting the intrusion in a system or a network. IDS is mainly classified into Host-Based Intrusion Detection System (HIDS), Network Intrusion Detection System (NIDS) based on the type of the systems the IDS protects. Signature Based Intrusion Detection System, Anomaly Based Intrusion Detection System are classified based on the method of working. HIDS analyses the incoming and outgoing packets from a system. This also monitors the operating system of the computer. NIDS monitors traffic on an individual network by continuously performing traffic analysis and then comparing it with detected or known attacks in the library. However IDS monitors mischievous activities, they might also generate False Alarms. Therefore the rate of False Alarms should be less when an IDS is implemented.

Detection of an intrusion starts where the firewall ends. Preventing unauthorized access is not in our hands. An intruder never leaves an opportunity to intrude into the network and cause damage to others information which leads to no privacy. These attacks are being increased every day.

Thus an intrusion detection system is needed to avoid such attacks. Many types of attacks can be detected with this intrusion detection system hence an intrusion detection system that has been designed or implemented needs to work efficiently to detect the attacks.

Log files record the behaviour of the computer system and aim at recording the action of the operating system, applications, and use behaviours. Log file is widely used for system debugging, monitoring, and security detection. Log system is particularly important in intrusion detection and log file analysis tools have become an indispensable tool for daily inspection and maintenance of the system running. In general, log analysis-based HIDS

includes the following several parts: collection of log file data, pre recording of log file, decoding of log file, analysis of log file and report events.

The HIDS combines two approaches of misuse detection and anomaly detection. Monitoring the log file, once the log changes, log monitor will send events to the log analyser immediately. Generally, we need to monitor three kinds of event logs: application log, security log and system log. We can add three XML nodes in the following configuration file. The node “local file” represents the local file when system initialization. The node “location” represents the file pathing the disk. The node “log format” represents what type of the log. Log type includes event log, firewall log, SQL log and so on. In this way, when initializing the HIDS, it will automatically load the above log files that need to be monitored. When finished the initialization work, the HIDS will open a demon, and the demon will check every log file to find whether there are changes in the log file. If there really exists change, then the demon will report to the log.

1.2: PROBLEM STATEMENT

There is enormous need for an efficient system that successfully detects and suggests a method to prevent the intrusions that occur across the network with a cost effective implementation, so as to ensure security to our data.

To accomplish this we need to implement an IDS - Intrusion Detection System

and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet.

Mobile ad-hoc networks became a popular subject for research as laptops and 802.11/Wi-Fi wireless networking became widespread in the mid- to late 1990s. Many of the academic papers evaluate protocols and abilities assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other, and usually with nodes sending data at a constant rate. Different protocols are then evaluated based on the packet drop rate, the overhead introduced by the routing protocol, and other measures.

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized; where all network activity including discovering the topology and delivering messages must be executed by the nodes.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem.

How to start TCL scripts?

We can write Tcl scripts in any text editor like joe or emacs. First of all, we need to create a simulator object. This is done with the command set ns [new Simulator] Now we open a file

OSSEC: It is one among the simplest open source applications. It's an incredibly efficient processor, but it doesn't have a user interface when it involves log data. It organizes your log files and uses anomaly based intrusion detection and it offers log file detection methods and scan for unauthorized changes could specifically cause issues.

SNORT: It is an open source NIDS application. It is 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 .

BLACK HOLE ATTACK

In computer networking, a packet drop attack or blackhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. One cause mentioned in research is through a denial-of-service attack on the router using a known DDoS tool. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.

The malicious router can also accomplish this attack selectively, e.g. by dropping packets for a particular network destination, at a certain time of the day, a packet every *n* packets or every *t* seconds, or a randomly selected portion of the packets. This is rather called a greyhound attack. If the malicious router attempts to drop all packets that come in, the attack can actually be discovered fairly quickly through common networking tools such as traceroute. Also, when other routers notice that the compromised router is dropping all traffic, they will generally begin to remove that router from their forwarding tables and eventually no traffic will flow to the attack. However, if the malicious router begins dropping packets on a specific time period or over every *n* packets, it is often harder to detect because some traffic still flows across the network.

The packet drop attack can be frequently deployed to attack wireless ad hoc networks. Because wireless networks have a much different architecture than that of a typical wired network, a host can broadcast that it has the shortest path towards a destination. By doing this, all traffic will be directed to the host that has been compromised, and the host is able to drop packets at will. Also over mobile ad hoc networks, hosts are specifically vulnerable to

collaborative attacks where multiple hosts will become compromised and deceive the other hosts on the network.

WORMHOLE ATTACK

This is a type of network layer attack which is carried out using more than one malicious node. The nodes used to carry out this attack are superior to normal nodes and are able to establish better communication channels over long ranges. The idea behind this attack is to forward the data from one compromised node to another malicious node at the other end of the network through a tunnel. As a result the other nodes in the WSN can be tricked into believing that they are closer to other nodes than they really are which can cause problems in the routing algorithm.Also the compromised nodes may temper with the data packets.

Wormhole attack can also be combined with sinkhole attack to make it more effective.

Wormhole attack can be classified under 3 main categories:

Open Wormhole:

In this case the data packets are first sent from the source to a wormhole which tunnels them to the other wormhole that transmits them to the destination.The other nodes in the network are ignored and not used for data transfer.

Half-open Wormhole:

In this case the data packets are sent from the source to a wormhole which directly transmits them to the destination.

Closed Wormhole:

In this case the data packets are directly transferred from the source to the destination in a single hop making them fictitious neighbours.