ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
June 2017,
Vol. 10, No. (2):
Pgs. 326-332

A New Distributed Intrusion Detection System in Computer Network: An Approach to Detect Malicious Intrusion Threats at Initial Stage

PARVEEN SADOTRA and CHANDRAKANT SHARMA

Department of computer Application, Career Point University, Kota, Rajasthan, India
Corresponding author e-mail: [1]Sadotramca2k6@rediff.com

http://dx.doi.org/10.13005/ojcst/10.02.10

(Received: March 15, 2017; Accepted: May 2, 2017)

ABSTRACT

Internet is a blessing for human community modern days and use of network is indispensable in present time. Use of networks and internet has also brought large numbers of security threats to our database and information systems. There are so many intrusion attacks on public and private networks. Main objective of this research work to study about problem associated with intrusion in network system and analyzes the use of intrusion Detection systems. Scrutinize the use of various IDS and develop a new IDS which should be most effective and easy to use also cost effective for users. So, we will be presenting our newly developed application based IDS which is to be suitable way to detect threat in the network system which can be cost effective and easy to use also it should have instantaneous alert system to notify intrusion to security professionals.

Keywords: IDS, DoS, NIDS, HIDS, DIDS

INTRODUCTION

In the recent decades with the rapid growth of the Internet and its related technology, many types of network and software applications have emerged. Also, same time, widely spread of Wide Area Network and Local Area Network application areas in many sectors of business such as industry, finance, security and healthcare sectors has made us more dependent on the computers. These application areas have made the network an attractive place to exploit, making the internet community more vulnerable.

Due to development of internet there are some bad characters whose challenge to do something becomes amusement for themselves whereas it becomes bad experiences for others. There are many cases when malicious acts which has made a nightmare to become a reality. And other than hacking, there are new things like worms, Trojans & viruses that have led to crisis

into the internet society. As we know that current situation is new, network security methods are weak. However, due to immense popularity of the Internet, computer connectivity and our manifold growing dependency on them, threat perception can have worst consequences. So, protecting such an important infrastructure of Internetworked devices has become our priority and this has become an interesting area of research in IT sector. Main purpose of this paper is to monitor and analyze current usage of Intrusion Detection Systems (IDS) along with analyzing some current problems that are present in this sector. In comparing to some mature and well settled research areas, IDS is relatively a new area of research. However, due to its importance and critical nature, it has attracted substantive attention of researchers towards it. We have seen researchers in this sector are rising rapidly. This new type of threat of intrusion into network is not just a probability that should be considered because it can happen any time. The currently whichever IDS s are used are far from reliability to protect our networks, but the main idea of Network security professionals should be to make it possible to find out novel network attacks and One of the major concerns is to make it sure that if there is an intrusion attempt, the system should be able to detect and report instantly. Once intrusion is detected our next step will be to protect the network. In other way, the IDS system should be upgraded to an Intrusion Detection and protection System. However, at present no part of the Intrusion Detection System fully reliable level. Even though researchers are presently giving their valuable time and are involved in working on both detection and protection of the networks.

About Intrusion Detection System

Intrusion detection systems (IDSs) are usually used along with other preventive security mechanisms, such as access control and authentication, as a second line of defense that protects information systems. There are many reasons behind making intrusion detection a necessity for the entire defense system. First, many traditional systems and applications have evolved without keeping security in mind. In other cases, systems and applications were developed to perform in a different environment and may become susceptible when deployed Intrusion detection complements these protective mechanisms to improve the system security. Moreover, even if the preventive security mechanisms can shield information systems successfully, it is still important to know what intrusions have taken place or which are ongoing, so that we can understand the security threats and risks and thus be ready for attacks in future.

The attack can happen in term of fast attack or slow attack. Fast attack can be termed as an attack that employs a large amount of packet or connection within a few second. Meanwhile, slow attack is as an attack that takes a few minutes or a few hours to complete. Both of the attack gives a great impact in the network environment due to the security breach decade., Currently IDS are used as a defensive tool in order to strengthen the network security especially in detecting the first two phases of an attack either in form slow or fast attack. An intrusion detection system can be divided broadly into two approaches which are behavior based that is anomaly and knowledge based that means misuse. The behavior based approach can also known as anomaly based system while knowledge based approach is known as misuse based systems. The misuse and/or signature based IDS is a system that contains a number of attack description or signature that are matched against a stream of audited data looking for various evidence of modeled attack. The audit report data can be gathered from network traffic or from and application log. This method can be used to detect previous known attack and the profile of the attacker has to be manually revised when new attack types are discovered. Hence, unknown attacks in network intrusion pattern and characteristic might not be capture using this technique meanwhile; the anomaly based system identifies the intrusion by identifying traffic or application which is presumed to be usual activity on the network or host. The error based system builds a model of the normal behavior of the system and then looks for erroneous activities such as activities that don't conform to the established model. Anything that does not correspond to the system profile is marked as intrusive. False alarms produced by both systems are a matter of great concern and it is taken as a key

problem. They also cause postponement of further implementation of reactive intrusion detection system.

Therefore, it is significant to decrease amount of false alarm generated by both of the system. Although false alarm is a major issue in developing the intrusion detection system especially the anomaly based intrusion detection system, yet the system has been able to meet fully the organizations' objective compared to the signature based system. The false positive generated by the anomaly based system is still tolerable even though expected behavior is identified as anomalous while

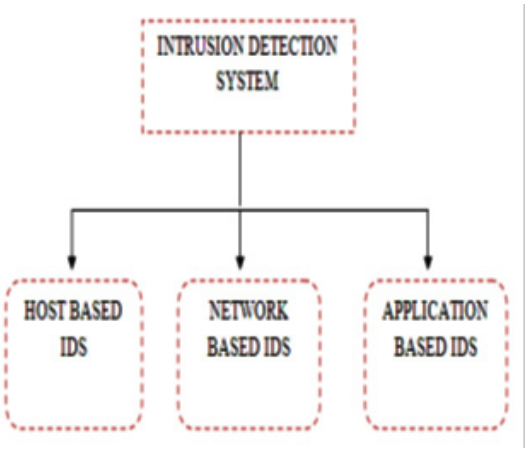

Fig. 1

false negative is not accepted because they do not detect an attack. An attack that deploys a large amount of packet or connection within a few second scanning attack, DoS attack, DDoS attack worm attack are some of fast attack Code Red Worm and NIMDA worm are another breed of DoS attacks on Internet infrastructure after the Morris Worm. Code Red Worm has a fast rate of propagation and infection via network scanning to detect and automatically exploit

NEED FOR INTRUSION DETECTION SYSTEM

When most people think of network security, they think, Firewall. Firewalls are widely deployed as a first level of protection in a multi-layer security architecture, primarily acting as an access control device by permitting specific protocols to pass between a set of source and destination addresses. Integral to access policy enforcement, firewalls usually inspect data packet headers to make traffic flow decisions. In general, they do not inspect the entire content of the packet and can't detect or thwart malicious code embedded within normal traffic. It should be noted that routers also offer some rudimentary protection through packet filtering processes.

While firewalls and router-based packet filtering are necessary components of an overall network security topology, they are insufficient on their own. Network IDS products inspect the

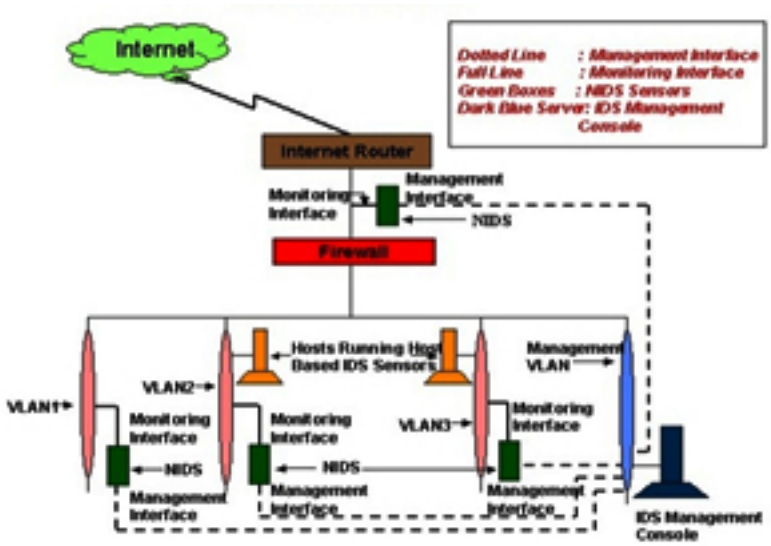

Fig. 2

entire content of every packet traversing the network to detect malicious activity. This content inspection technique provides deeper packet analysis compared to a firewall or a router. Intrusion Detection Systems are effective when sophisticated attacks are embedded in familiar protocols, such as an HTTP session, which would normally pass undetected by a firewall. It's not surprising that the processing power required for an Intrusion Detection System is an order of magnitude higher, when it is compared with firewall product.

Permeable modern networks have made IDS products necessary tools for security engineers to detect, analyze and defend networks against malicious threat. As a result, IDS machines are being deployed outside and inside firewalls and are rapidly becoming popular in best practice to secure network implementations.

objective of the present work

The first step in securing a networked system is to detect the threat of intrusion. Even if the system cannot prevent the intruder from getting into the system, noticing the intrusion will facilitate the security experts with crucial information. The Intrusion Detection can be considered to be the start point of defending any network system.

types of ids

Three types of IDS are present there

- Host based
- Network based
- Application based

Host Based Intrusion Detection System HIDS views the sign of intrusion in the local network system. For analysis, they use host system's logging and other information.

Advantages

- HIDS verifies success or failure of a threat
- HIDS Monitors activities of the System
- HIDS detects attacks when a network based IDS fails to detect
- HIDS has almost real time detection and response
- HIDS does not require any additional hardware
- HIDS has lower cost

Network based IDS systems

NIDS collect information from the network itself rather than from each different host. The NIDS audits the network attacks while packets moving all over the network.

Advantages

- NIDS has lower Cost of Ownership
- NIDS is easier to use
- NIDS detects all the network based attacks
- NIDS retains all evidences
- NIDS has real time detection and quick response.

IDS based on Application (APIDS)

APIDS system is installed between a process and servers or group of servers that monitors and analyzes the application protocol between various devices. Intentional attacks which are deadly attacks in nature, carried out by frustrated staff of the organization to harm to the organization. Unintentional attacks are the attacks which causes monetary losses to the organization by manipulation of significant data file.There are so many attacks that have taken place in OSI layer of network.

Ids Setup In Network

Analysis Of Present Idss

After going through existing IDS, we could analyze and see that none of present Intrusion Detection Systems are capable enough to detect all kinds of network penetration. There are so types of IDS but none of them can be relied 100 %. There are many companies which boast about their IDS that they are capable of giving accurate and reliable intrusion alert but our scrutiny into those IDS gave a glance that there is no IDS as on date which can be complete security solutions as per our needs. Every IDS has its advantage and disadvantages and we have to compromise somewhere at some time.

Proposed New Ids

After analyzing various types of IDS, we have developed a new kind of IDS which is be a software and application based. This IDS can perform log analysis and can check for file integrity, it can monitor various policies, detect rootkit if any, give alert on real-time basis and there will be active

response. It can be run on all platforms viz Windows, Linux, Polaris also on Mac. This IDS can keep eyes on data travelling on our networks and will give alerts to network admin in case of any irregularities. It will also keep a detailed log which will provide us with detailed information about what has happened in our network system so that a decision can be made to prevent damage to our systems

Algorithm And Coding Of Proposed Ids

We propose the IDS system which have following modules: -

Various Modules In New Ids

The first module is responsible for capturing all live packets from network. All the packets which are captured are to be passed to next module which is called *Packet Preprocessing Module*. Packet preprocessing module classifies all the captured packets as per various protocol e.g. TCP/IP, UDP, HTTP etc. Finally these packets are send to next module called as *Intrusion Detection Module*. Here This module checks for all intrusions. If the packet is unknown and intruder then the detector makes a log of attack & generates intrusion alarm.

Intrusion Detection Module

Multi-threading programming feature is present in the Intrusion Detection Module, which allows several threads to exist within the context of one single process. The Model of threaded programming is very useful as it provides an important abstraction of concurrent execution. So, to deal with such problems we are proposing a multithreaded design.

Below is the algorithm being is used in order to solve the problem using multithreaded technique

Algorithm Multithreading

As you can see here, *capturedPacketCount* keeps track of all the captured packets and *threadCount* will be responsible to count the number of threads being created in Detection process, whereas capacity (N) is a variable which holds the max number of packets in a single thread that can be handled. *ThreadCount* is initialized to 1 as first thread will be created and it will wait for first packet. After that it will handle up to N packets. After N packets, new thread will be created to handle further packets i.e. second thread will handle packets from N to 2N and third thread will be responsible to handle packets from 2N to 3N and like this so on.

Components of Agent

Figure at below shows different modules of agent. There are three modules in agent: -

Figure: Module Agents

Database of Frequent Attack Signature

we have a database of huge number of signatures for the methods of signature based intrusion detection. It facilitates to check if the packet which is incoming is an intruder packet or not, here we match the signatures of all the incoming packets with signatures that are present in our database. But this process is very time consuming so to overcome this problem, we will use a mechanism which is called as cache mechanism. We will maintain a cache of database of all frequent occurring intruding signatures. And complementary holds all the signatures in the database.

Detection Module

The main component of agent is detection module. This module has main task to detect an intrusion. This module works as follows.

The detection Module takes all packets as input and extracts their signature. These extracted signatures are being compared with all the signatures present in the cached database first, in order to check any intrusion. If there is any match, then that particular packet is marked as intruding

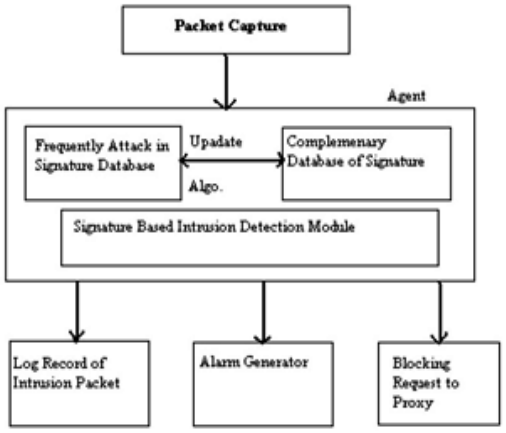

Fig. 3

packet which results to detection of intrusion in a very short time. And if there is no matching of signature then the extracted signature will be compared with all the signatures that are present in complementary database. If match occurs here, then packet is categorized as intruding packet else that is categorized as a normal packet. This module also integrates multithreading logic system as discussed above.

Module for Updating signature database

This module is responsible for keeping database of signatures up-to-date.

Algorithm

For Module Updation implementation Features and Advantage of Our IDS

There are following advantages of using newly developed IDS by us

- Our proposed IDS is aware of specific users and has capability to observe the interaction between various Applications and users.
- It will allow the IDS to stop illegal activities to specific and already known users of the network.
- We can get alerts of intrusion even though, we are on move in the form of text message to our mobile phone linked to IDS.
- New IDS will be able to operate in the conditions where the data is encrypted.

As Internet usage by human society is increasing rapidly same time Intrusion to networks too increasing drastically. We have employed Network security experts, we developed various kinds of Intrusion Detection Systems of various types. Technological improvement has enabled us to protect our networks from miscreants but this is a never-ending process because whatever ways we find to protect us hackers find a new way to crack it.

We studied various kinds of IDS present in present days. Every IDS has its pros and cons and none of them is 100 % secured. Use of IDS is indispensable in present unprotected networks in order to protect them from external threat. Based on the problems in the existing IDS, we developed and proposed a new application based IDS which will be economical to use for everyone and this IDS is one way an assurance for better detection of intrusion to network thus enabling security experts for better decision making and ultimately, we can say it will be providing a new dimension to securing our networks.

REFERENCES

1. J. Allen et al., *State of the Practice of Intrusion Detection Technologies*, Tech Report CMU/ SEI-99-TR-028, Carnegie Mellon Univ., Software Engineering Inst., Pittsburgh, 2000
2. Jennifer Jabbusch , “IDS vs. IPS: How to know when you need the technology”, 22 November 2010
3. Kent, Karen & Warnock, Matthew (2004). *Intrusion Detection Tools Report, 4th Edition.* Herndon, VA: Information Assurance Technology Analysis Center (IATAC).
4. Pete Lindstrom, “Intrusion prevention systems (IPS): Next generation firewalls”, A Spire Research Report – March 2004 by, Spire Security
5. Parveen Sadotra(CEH) and Dr. Chandrakant Sharma, “Transformation in Building More Intelligent Intrusion System: A review” presented in *ICEECSIT- 17 at New Delhi, India, PP. 1 - 5*
6. Debar, H., An Introduction to Intrusion Detection Systems, IBM Research, Zurich Research Laboratory
7. Jan Vykopal, “Security Analysis of a Computer Network”, Masaryk University Brno, master thesis, 2008.
8. Charlie Kaufman, Radia Perlmon and Mike Speciner; Network Security; Private Communication in a Public World, 2nd Edition, Prentice Hall of India
9. William Stallings, Cryptography and Network Security: Principles and Practices, Pearson Education, 4th Edition, 2011.
10. Jeevaa Katiravan, C. Chellappan and J. Gincy Rejula Detecting the Source of TCP

SYN Flood Attack using IP Trace Back European Journal of Scientific Research ISSN 1450-216X Vol.**71** No.1 (2012), pp. 78-84

11. V. Jyothsna, V. V. Rama Prasad and K. Munivara Prasad "A Review of Anomaly based Intrusion Detection Systems" International Journal of Computer Applications (0975 – 8887) Volume **28**– No.7, August 2011
12. Asmaa Shaker Ashoor and Prof. Sharad Gore "Importance of Intrusion Detection System (IDS)" International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011 ISSN 2229-5518
13. Firkhan Ali Bin Hamid Ali and Yee Yong Len "Development of Host Based Intrusion Detection System for Log Files" IEEE symposium on business, engineering and industrial application(ISBEIA) langkawi, malaysia 2011
14. Chung-Ming Ou and C.R. Ou "Immunity-inspired Host-based Intrusion Detection Systems" 2011 Fifth *IEEE International Conference on Genetic and Evolutionary Computing.*
15. Ferdous A. Barbhuiya, Santosh Biswas, Neminath Hubballi and Sukumar Nandi "A Host Based DES Approach for Detecting ARP Spoofing" IEEE Conferences 2011
16. Bin Zeng, Lu Yao, ZhiChen Chen "A Network Intrusion Detection System with the Snooping Agents" *IEEE International Conference on Computer Application and System Modeling* (ICCASM 2010) 2010.
17. LIN Ying, ZHANG Yan and OU Yang-Jia "The Design and Implementation of Host-based Intrusion Detection System" Third IEEE *International Symposium on Intelligent Information Technology and Security Informatics* 2010
18. Anuradha and Anita Singhrova A Host Based Intrusion Detection System for DDoS Attack in WLAN IEEE *International Conference on Computer & Communication Technology* (ICCCT)-2011
19. Chundong Wang, Quancai Deng, Qing Chang, Hua Zhang and Huaibin Wang " A New Intrusion Detection System Based on Protocol Acknowledgement" IEEE 2010
20. Parveen Sadotra *et al*, A Review on Integrated Intrusion Detection System In Cyber Security *International Journal of Computer Science and Mobile Computing*, Vol.5 Issue.9, September- 2016, pg. 23-28.
21. M.A., Faizal, Mohd Zaki M., Shahrin Sahib, Robiah Y., Siti Rahayu S., and Asrul Hadi Y.. "Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System", 2010 Second International Conference on *Network Applications Protocols and Services*, 2010.
22. Parveen Sadotra and Chandrakant Sharma. A Survey: Intelligent Intrusion Detection System in Computer Security. *International Journal of Computer Applications* 151(3):18-22, October 2016.
23. Fessi, B.A.. "A decisional framework system for computer network intrusion detection", *European Journal of Operational Research*, 20070316