IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THREATS IN NETWORK INTRUSION DETECTION SYSTEM

Mr. Thamraj Narendra Ghorsad
Phd Scholar, Computer Science & Engineering Department,
G. H. Raisoni University Amravati,

Prof. Rais Abdul Hamid Khan,
Professor, Computer Science & Engineering Department,
G. H. Raisoni University Amravati

***Abstract*— Network Intrusion Detection System (NIDS) defined as a Device or software application which monitors the network or system activities and finds if there is any unwanted activity occurs.Outstanding development and usage of internet raises concerns about how to communicate and protect the digital information safely.In today's world hackers use Variety of attacks for obtainingthe valuable information. Most of the intrusion detectiontechniques, methods and algorithms help to detect those several attacks. The main motive of this paper is to provide a complete study about the intrusion detection, variety of intrusion detection methods, variety of attacks, different tools and techniques, research needs, challenges and finally develop the IDS Tool for Research Purpose That tool are capable of detect and prevent theintrusion from the intruder.**

***Index Terms*—Network Intrusion Detection System, Need, Type of NIDS, Detection Techniques, Functioning of NIDS, Components, Application based NIDS, Tools of NIDS.**

I. INTRODUCTION

At the present time internet security has become a challenge for organisations. To protect credential data from the intruders. In process of safeguard the data Web Firewalls, encryption, authentication and Virtual Private Networks (VPN) have been deployed since a long time to secure the network infrastructure and communication over the internet. Intrusion detection is a relatively inclusion to set of security technologies.

NIDS is an evolution which enhance the network security and protect the data of the organisation. The NIDS helps the network administrator to detect any unwanted activity on the network and attentive the administrator to get the data secured by taking the appropriate actions against those attacks.

An intrusion refers to any unauthorized access or unwanted utilization of information appliances. An intruder or an attackeris a reality entity that tries to find a means to gain unauthorized access to information causes harm or engage in other unwanted activities.

The Network intrusion detection system is about the firewall security. The firewall safeguard an organization from the unwanted attacks from the Internet and the NIDS detects if someone tries to access in through the firewall or manages to break in the firewall security and tries to have an access on any system in the organization and attentive the system administrator if there is an undesired activity in the firewall.

Therefore, an Network intrusion detection system (NIDS) is a securitysystem that monitors network rush and computer systems and works to analyse that rush for possible hostile attacks originating from outside the organization and also for misapply of system or attacks originating from inside the organization.

II. NEED

These days internet has become part of our daily life infect, the business world is obtaining connected to Internet.Number of peoples are obtaining connected to the Internet every day to take advantage of the new business model which is known as e-Business. Connectivity improvement has thereforebecome very censorious aspect of today's e- business.

There are two stages of business on the Internet. First phase is the Internet brings in Excellent potential to businessin terms of reaching the users and at the same time it also brings a lot of risk to the business. There are both safe and damaging users on the Internet. Whereas an organization makes its information system accessible to safe Internet users. Unwanted users or

hackers can also get an access to organization's internal systems in various reasons. These are,

- Software bugs called vulnerabilities in a system
- Failure in administration security
- Leaving systems to default configuration

The intruders are use distinct types of techniques like Password cracking, peer-to-peer attack, Sniffing attack, Dos attacks, Eavesdropping attack, Application layer attack etc. to exploit the system vulnerabilities mentioned above and compromise censorious systems. Therefore, there required to be some kind of security to the private appliances of the organization from the Internet as well as from users inside the organization.

III. VARIETY OF NETWORK INTRUSION DETECTION SYSTEMS:

There are two varieties of Network intrusion Detection systems. These are network based intrusion Detection System and host based intrusion Detection System.

1. Network Based Intrusion Detection and Prevention System

A Network Based IDS (NIDS) present in a computer or device connected to a segment of an organization's network and monitors network rush on that network segment, looking for ongoing attacks. In network for maintain security to files many various Hashing algorithms are used like MD5. When a circumstances happens that the network-based IDS is planned to know an attack, it responds by sending notifications to administrators. NIDS looks for attack patterns within a networkrush, such as large sets of related items that are of a certain type that could specify that a denial-of-service attack isongoing, or it looks for the interchange of a order of related packets in a certain pattern, which could indicate that a port scan is in progress. NIDSs are installed at a specific place in the network (router is one of example) from where it is possible to see the rush going in and beyond a particular network segment and it can be used as watch the specific host computers on a network segment, or it can be installed to monitor all rush between the systems that make up an entire network.

2. Host Based Intrusion Detection System

A Host Based Intrusion Detection System (HIDS) is placed on a specific computer or server, known as the host, and monitors activity only on that system. Host based intrusion detection systems can be further split into two categories: signature-based (i.e. misapply detection) and anomaly based detection techniques. HIDS keep track of the status of key system files and discover when an intruder creates, modifies, or deletes the monitored files. Then the HIDS triggers an attentive when one of the following changes appears: file attributes are changed, new files are created, or existing files are deleted. The main dissimilarity between NIDS and HIDS is that the NIDS canenter information that is encrypted when traveling through thenetwork.

A. Usefulness of HIDS

HIDS can discover local events on host systems and also discover attacks that may avoid network-based IDS.

HIDS encoded rush will have been decoded and isavailable for processing.

The use of switched network protocols does not influence a HIDS.

IV. INTRUSION DETECTION TECHNIQUES

The two varieties of IDS techniques are:-

A. ABD Technique: An anomaly- based intrusion detection system, is a technique for detecting both network and computer intrusions and misapply by monitoring system activity and classifying it as either normal or anomalous. The classification is based on some rules, alternately patterns or signatures, and attempts to detect any type of unwanted activity that falls out of normal system operation. While the signature- based systems can only discover attacks for which a signature has earlier been created.

A. Advantages of this anomaly detection method

The chances of detection of novel attacks as intrusions; anomalies are recognized without obtaining inside their causes and characteristics; less dependence of IDS on operating environment (a compared with attack signature- based systems); capacity to discover abuse of user privileges.

B. SIGNATURE BASED INTRUSION DETECTION:

Signature-based IDS refers to the find out of attacks by looking for specific patterns, such as byte sequences in network rush, or known unwanted instruction sequences used by malware. The terminology is produced by anti- virus software, which refers to these detected patterns as signatures. Even though signature-based IDS can easily discover known attacks, it is impossible to discover new attacks, for which no pattern is available.

This technique automatically possess the signature to discover the intruder. Misuse detection technique is created automatically and the works are more complicated and accurate than manually done. It will Depending on the robustness and seriousness of a signature that is activated within the system,

some alarm response or notification should be sent to the right authorities.

V. FUNCTIONS OF IDS

The IDS consist of four main functions namely, data collection, feature selection, analysis and action,

Figure1: Functionality of IDS

1. 1. Data collection: This module moves the data as input to IDS. The data is recorded into a file and then examine. Network based IDS collects and changes the data packets and in host based IDS collects details likeusage of the disk and processes of system.
   2. Feature Selection: To select the specific feature large data is available in the network and they are usually evaluated
   3. for intrusion. For example, the Internet Protocol (IP) address ofthe source and destination system, protocol type, header lengthand size could be taken as a key for intrusion choice.

1. Analysis: The data is examined to find the correctness. Rule based IDS analyse the data where the incoming rush is checked against predefined signature or pattern. Another method is anomaly based IDS where the process of system is studied and mathematical models are employed to it.

2. Action: It defines about the response and attack of the system. It can either inform that the system administrator with all the essential data through an email/alarm icons or it can playan active part in the system by dropping packets therefore it doesnot admit the system or close the ports.

VI. COMPONENTS OF AN INTRUSION DETECTION SYSTEM

There are three fundamental components of an IDS – Sensor (Activity or packet capture engine, Behavioural or signature detection engine), Backside (Event recording of database, attentiveing the engine) and the Frontside (User interface, Command & control).A sensor set up the primary component of an IDS for detecting intrusions on a computer or a network. It capture a packet to perform detection activities. It can employ the signature based or anomaly based IDT. The backend of the IDS is related with logging of events which is detected by the sensors. Additionally, it performs the function of attentiveing. The backendcan attentive the administrator in frequent ways – logging events inthe database, sending an e-mail, block a connection, reset a TCP connection, and display the attentive on the administrator's console. The frontend forms the IDS user interface. The user can see events that the sensor has detected, setup the IDS,update the signature database and behavioral detection engine.

VII. WORKING OF AN INTRUSION DETECTION SYSTEM

The components of an IDS work in a structured manner to attentive the administrator of an intrusion.

A. Sensor – It is divided into two types firstly, the capture network interface and secondly, the management network interface.Its main function is Detect and Report. As the sensor hear ɒ network rush by draining toward the network, the capture interface passes on all the captured data into a buffer. Thenthe detection engine checks the buffer contents and executes network protocol analysis. based on Signature and based on anomaly, based on intrusion detection also occurred here.

B. Backend - The backend is also call as the main function of an IDS. Its main function is combine and attentive. The events discover by the sensor are recorded in the event repository database system. Then the backend determines how each event has to be responded to E-mails, displays, blocking are used to respond to censorious events.

C. Frontend- Command and Control the intrusion detection system can be setup, configured and updated from the frontend by the user. Every events gathered by the backend are presented on the frontend. Thus, the frontend supplies a suitable interface through which the user can now manage these logged events. To obtainmaximum benefit from IDS, it has to be adjusting to reportonly significant events. Hence, the user can adjust the detection and response of IDS through this

console. If done with accuracy, the IDS will supplies the user with adequately early warning from any intrusion.

VIII. APPLICATION BASED IDS (APIDS)

APIDS will examine the practical behavior and event of theprotocol. The system or agent is placed between a process and set of servers that monitors and analyses the application protocol between devices. Intended attacks are the hostile attacks carried out by malcontent employees to cause harm to the organization and Unintentional attacks causes financial damage to the organization by deleting the important data file. There are number of attacks have been taken place in OSI layer.

Denial-of-Service (DOS) Attacks: DOS mention to Denial-of-Service and is best defined as an attempt to make a computer(s)or network(s) unavailable to its intended users or also a Denialof Service attack is when an attacker is trying to produce morerush than you have appliances to handle.

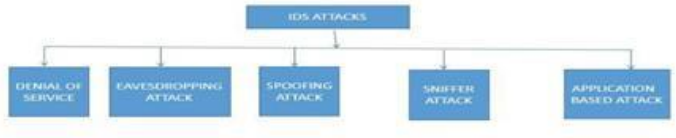
DOS and DDOS: In a DOS attack, one computer and one internet connection also is established to overwhelm a server or network with data packets, with the only intention of overloading the bandwidth of victim and available appliances. ADistributed Denial of Service (DDOS) attack is the same, but itis amplified. Alternately one computer and one internet connection a DDOS is, and often involves millions of computers all being used in a distributed manner to have the effect of hitting a web site, web application or network offline.

In both cases, either by the DOS or the DDOS attack, the destination is bombarded with data entreaties that have the effect of disabling the functionality of the victim.

SYN Attack: SYN attack is also defined as Synchronizationattack. Here, the attacker sends the flood of SYN entreaty to the destination to utilize the appliances of the server and to make the system passive.

Peer-to-peer assault : A P2P network is a distributed network in which individual nodes in the network called “peers” act as both suppliers (seeds) and consumers (leeches) of appliances, in difference to the centralized client– server model where the client server or operating system nodes entreaty access to appliances provided by central servers.

Ping of Death: A type of DOS attack in which the attacker deliver a ping entreaty that is larger than 65,536 bytes, which is the maximum size that IP allows onto the network. While a ping larger than 65,536 bytes is Excessively large to fit in one packet that can be transmitted through, TCP/IP allows a packet to be fragmented, essentially splitting them in smaller segments that are reassembled at the end point. Attacks took benefit of this limitation by breaking up packets that when received packet would total more than the allowed number of bytes and would effectively cause a buffer overload on the operating system at the receive side then the system could accident.



Eavesdropping Attack: It is the scheme of intervention in communication by the attacker. This attack can be done over by telephone lines, immediate message or through email.

Identity Spoofing (IP Address Spoofing): Most operating systems and networks utilize the IP address of a computer to identify a valid entity on the network. In some cases, it is feasible for an IP address to be falsely considered have spoofingidentity. An attacker might also use particular programs to build IP packets that are originate from valid IP addresses inside the corporate intranet. After entrance to the network with a valid IP address, the attacker can alter, re-routing, or deleting your data.

Man-in-the-Middle Attack: As the name suggests, a man- in-the-middle attack appears when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communicationtransparently. For example, the assailant can re-route a data exchange. When computers are communicating at lowest levelsof the network layer like physical layer, the computers might not been able to decide with whom they are exchanging the data. Man-in-the-middle attacks are like someone consideringyour identity in order to read your message. The person on the other side might believe as it is you by reason the attacker might be actively replying as you to keep exchanging the information.This attack is able of the same harm as an application layer attack, which is described below.

Application Layer Attack: An application-layer attack targeted application servers by intentionally causing a fault in a server's OS or applications. This results in the attacker obtaining the ability to bypass accessing normal controls. The attacker takes benefits of this situation, obtaining control of

your application, system, or network, and can do some of the below:

- Read, add, delete, or alter your data or operating system.
- Can say about a virus program that utilizes your computers and software applications to copy viruses throughout entire network.
- Can say about a sniffer program to analyze your network and gain details that can be used to crash or to corrupt your systems and network.

• Uncommonly finished your data applications or operating systems and Disable other security controls to enable future attacks.

Sniffer Attack: A sniffer is an application or device that canobserve, read, and capture network data exchanges and read network packets. If the packets are not encoded, a sniffer provides a full view of the data inside the packet.

IX. TOOLS OF INTRUSION DETECTION

An intrusion detection product accessible today addresses a range of organizational security goals. The security tools.

SNORT: Snort is lightweight and open source software. Snort uses a flexible rule-based language to describe the rush from an IP address; it records the packet in human readable form through protocol analysis, content searching, and variouspre-processors Snort discovers thousands of worms, vulnerabilityexploit attempts, port scans, and other suspicious behavior.

OSSEC-HIDS: OSSEC (open source security) is free open source s/w. It will run on major operating systems and utilize a Client/Server based architecture. OSSEC has the capacity to dispatch OS logs to the server for analysis and storage the data. It is used in several powerful log analysis engine, ISPs, universities and data centres Authentication logs, firewalls are monitored and analysed by HIDS.

KISMET: It is a direction for Wireless intrusion detection system.WIDS compromises with packet payload and happenings of WIDS. It will find the burglar access point.

Installing IDS: Simple and easy we implement IDS in two models which is:

➔ Two models are:

- Local (when you have just one system to monitor)
- Client/Server for centralized analysis (recommended!)

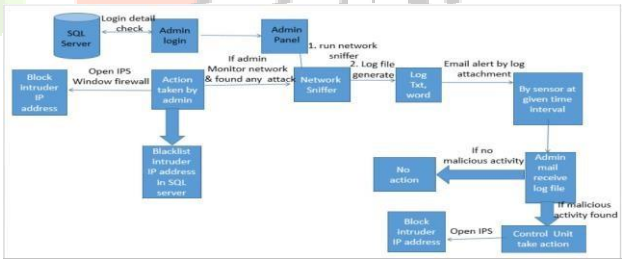
Functioning of IDS Tool: IDS is a Host based intrusion detection System/intrusion prevention System Tool in which we can monitor input and output data packets or rush from the device and using this tool administrator also performs log analysis they find the pattern of attack into the logs if any unwanted attack pattern found like UDP FLOOD which is the type of Dos assault so administrator inform to control unit they will take action against those attack they will block the IP address of intruder and store the intruder information in SQL Server and also trace the intruder IP Address so finally we detect and prevent the intrusion.

Component of IDS:

1. 1. Network sniffer: A packet analyser (also known as a packet sniffer) is a piece of software or hardware designed to intercept data as it is transmitted over a network and decrypt the data into a format that is understandable for humans.

   As data streams flow beyond the network, the sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet.
2. 2. Recognise intrusion using log based analysis: Those packets which is received by network sniffer is stored in a log file. These log file are used for analyse the network rush by the administrator if any unwanted activity or attack found in this log file then administrator inform control unit they will take action in opposite to those attacks and these log file will be usedfor forensic purpose in future.
3. Sensor: Sensor reports the administrator by dispatching email with log file and admin analyses those log file and take action if any attack will found so they inform to the control unitand they will take action against those attacks.
4. Control Unit: The Control Unit takes action againstintruder attack they will block the IP address of the intruder in the firewall of the system and store the information aboutintruder in SQL server and blacklisting the intruder IP address by using SQL server and also trace the intruder IP address.

IDS Architecture:



CONCLUON

NIDS are becoming the main part for many organizations after deploying firewall technology at the network perimeter. NIDS can offer protection from external users and internal attackers, where rush doesn't go past the firewall at all. However, the below points are must to always keep in mind.If all of these points are not attached to, an IDS implementationalong with a firewall alone cannot make a highly secured infrastructure.

1. Strong identification and authentication: An IDS uses very good signature analysis mechanisms to detectintrusions or potential misapply; however, organizations must still ensure that they have strong user identification and authentication mechanism in place.
2. Intrusion Detection Systems are not a solution to all security concerns: IDS perform an excellent job of ensuring that intruder attempts are monitored and reported. In addition, companies must employ a process of system testing, employee education, and development of and attached to a good security policy in order to minimize the intrusions risks.
3. An IDS is not a substitute for a good security policy: As with good security and monitoring products, an IDS functions is one element of a corporate security policy. Successful intrusion detection requires that a well- defined policy must be followed to ensure that vulnerabilities, intrusions and virus outbreaks, etc. are handled according to corporate security policy guidelines.
4. Human intervention is required: The securityadministrator or network manager must investigate theattack once. It is detected and reported, determine how it has occurred, correct the problem and take the necessary actions to prevent the occurrences of the same attacks in future that might happen

REFERENCES

[1] Salvatore Pontarelli, Giuseppe Bianchi, Simone Teofili. Rush-aware Design of a High Speed FPGA Network Intrusion Detection System. Digital Object Indentifier 10.1109/TC.2012.105, IEEE TRANSACTIONS ON COMPUTERS.

[2] Przemyslaw Kazienko & Piotr Dorosz. Intrusion Detection Systems (IDS) Part I - (network intrusions; attack symptoms; IDS tasks; and IDS architecture). www.windowsecurity.com › Articles & Tutorials

[3] Sailesh Kumar, "Survey of Current Network Intrusion Detection Techniques", available at http://www.cse.wustl.edu/~jain/cse571-07/ftp/ids.pdf.

[4] Srilatha Chebrolu, Ajith Abrahama,,*, Johnson P. Thomas, Feature deduction and ensemble design of intrusion detection systems, Elsevier Ltd. doi:10.1016/j.cose.2004.09.008

[5] Uwe Aickelin, Julie Greensmith, Jamie Twycross .Immune System Approaches to Intrusion Detection - A Review.http://eprints.nottingham.ac.uk/619/1/04icaris_ids _ review.pdf

[6] http://www.intechopen.com/download/get/type/pdfs/id/86 9 5.

[7] Martin Roesch , "Snort – Lightweight Intrusion Detection for Networks", © 1999 by The USENIX Association.

[8] The Snort Project, Snort User Manual 2.9.5,May 29, 2013, Copyright 1998-2003Martin Roesch, Copyright 2001- 2003 Chris Green, Copyright 2003-2013 Sourcefire, Inc.

[9] Chapter 3, Working With Snort Rules, Pearson Education Inc.

[10] B. Daya ,"Network Security: History, Importance, andFuture ,"University of Florida Department of Electrical and Computer Engineering , 2013. http://web.mit.edu/~bdaya/www/Network%20Security.pdf

[11] Li CHEN,Web Security : Theory And Applications,Schoolof Software,Sun Yat-sen University, China.

[12] J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library, 2000.

[13] A. R. F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University, 2010.

[14] S. A. Khayam, Recent Advances in Intrusion Detection, Proceedings of the 26th Annual Computer Security Applications Conference, Saint-Malo, France, pp. 224-243, 42, 2009

[15] M. M. B. W. Pikoulas J, "Software Agents and Computer Network Security," Napier University, Scotland, UK.

[16] R. E. Mahan, "Introduction to Computer & Network Security," Washington State University, 2000.

[17] Q. Gu, Peng Liu, "Denial of Service Attacks," Texas State University, San Marcos.

[18] M. A. Shibli, "MagicNET: Human Immune System & Network Security," IJCSNS International Journal of Computer Science and Network Security,Vol. .9 No.1, January 2009.

[19] M. Eian, "Fragility of the Robust Security Network: 80211," Norwegian University of Science and Technology, 2011.

[20] D. Acemoglu, "Network Security and Contagion," NATIONAL BUREAU OF ECONOMIC RESEARCH, 2013.

[21] J. Xu, J. Wang, S. Xie, W. Chen and J. Kim, "Study on Intrusion Detection Policy for Wireless Sensor Networks", International Journal of Security and Its Applications, vol. 7, no. 1, (2013) January, pp. 1-6.

[22] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: a Survey", Computer Networks, vol. 38, no. 4, (2002), pp. 393-422.

[23] K. Martinez, J. Hart, and R. Ong, "Environmental Sensor Networks", IEEE Computer, vol. 37, no. 8, (2004), pp. 50-56.

[24] R. Abouhogail, "Security Assessment for Key Management in Mobile Ad Hoc Networks", International Journal of Security and Its Applications, vol. 8, no. 1, (2014), pp. 169-182, http://dx.doi.org/10.14257/ijsia.2014.8.1.16,.

[25] E. Ngai, J. Liu, and M. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks", IEEE International Conference on Communications, (2006).

[26] D. Martins and H. Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", 13th International Conference on Network-Based Information Systems, (2010).

[27] M. Jain, "Wireless Sensor Networks: Security Issues and Challenges", International Journal of Computer and Information Technology, vol. 2, no. 1, (2011), pp. 62-67.

[28] N. Sethi and D. Sharma, "A Novel Method of Image Encryption Using Logistic Mapping", International Journal of Computer Science Engineering, vol. 1, no. 2, (2012)

November.

[29] S. Karmakar and S. Chandra, "An Approach for Ensuring Security and its Verification", International Journal of Computer Science Engineering", vol. 2, no. 3, (2013) May.

[30] M. Dinesh and E. Redddy, "Ultimate Video Spreading With Qos over Wireless Network Using Selective Repeat Algorithm" International Journal of Computer Science Engineering, vol. 2, no. 4, (2013) July.

[31] D. Carman, P. Krus, and B. Matt, "Constraints and Approaches for Distributed Sensor Network Security", Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, (2000).

[32] J. Sen, "A Survey on Wireless Sensor Network Security", International Journal of Communication

[33] Kang Hong, Zhang Jiangang, — An Improved Snort Intrusion Detection System Based on Self-Similar Rushmode ‖, Computer Network and Multimedia Technology, 2009. CNMT 2009. International Symposium on, 18-20
Jan. 2009.

[34] Zhimin Zhou, Chen Zhongwen, Zhou Tiecheng, Guan Xiaohui, — the Study on Network Intrusion Detection System of Snort, Networking and Digital Society (ICNDS), 2010 2nd International Conference on (Volume:2), 30-31, May 2010.