International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 07 | July 2019 www.irjet.net p-ISSN: 2395-0072

A Review on Intrusion Detection System

Pushpa Bharti Singh[1], Dr. Urvashi Chugh[2], Dr. Madhumita Kathuria[3]

[1,2,3]*Department of Computer Science Engineering and Technology Manav Rachna International Institute of Research and studies, (MRIU)), Faridabad, India*

***Abstract* — the vital and essential objective of intrusion detection is to supervise the network goods and valuables to uncover anomalous behavior and exploitation in the network. Intrusion Detection System is a network framework which has the potential of learning from records about previous attacks to recognize newly introduced attacks. By using IDS, we gather and use information from acknowledged attacks and find out attack into the network/host. Nowadays, cybercriminal implements numerous varieties of attacks for accessing confidential data and resources. Many intrusion detection techniques, methods, and algorithms give assistance to detect these attacks. The main objective of this study is to provide a complete analysis of intrusion detection system evolution and working life cycle of IDS with the classification of intrusion detection methods including various kinds of attacks also different tools available to prevent intrusions and however it also gives clear comparison between existing firewall security system and IDS with challenges and issues.**

Keywords—Intrusions, Anomaly and Signature Detection, Taxonomy, IDS Evolution, Tools

I. INTRODUCTION

In today's technical world networks are used by millions of internet users for storing and sharing audios, videos, text, and images and also for discussing their day to day activities, so security is a major concern that should be taken care of [4]. As millions of users are migrating toward internet services, it also attracting attackers and hackers or illegal traders to introduce vulnerabilities into the network to create loopholes in data centers or applications .which makes difficult to identify intruder in a network and become easy for them to escape. So we need a robust system for detecting and identifying intrusions called Intrusion detection a system. Idea of Intrusion detection was came in existence after the improvement of internet threat monitoring system concept introduced in 1980[14].

Basically intrusions are collective actions performed to break the security of the system. Intruders may be as of exterior the system or genuine clients. Occurrence of Intrusion can take place on any of three levels physical level, system level or remote level. Intrusion makes system being compromised and allows the vulnerabilities to enter into it [19].This leads to give control of host machine to a attacker or hacker. Who can manipulate, modify, destroy or misuse these system files. The concept of Intrusion Detection was introduced in 1980 by J.P. Anderson [1] Moreover, Firewalls plays a vital role in filtering all the incoming and outgoing network traffic .If users outside the organization network wants to connect to the internal network they can do so through dialing in via installed modems inside the organization. These accesses to the intranet can't be recognized by firewall [15]. So we are required to use a software like IDS that is installed on a system, which will be active all the time to detect and prevent it from malicious intrusion. It can detect intrusions which weren't blocked by other robust preventive technique like firewalls, routers, packet-filtering proxy servers.

II. PRINCIPLES AND THE TERMINOLOGY OF IDS

- An IDS must run unattended for extended period of time.
- The IDS should be operative, functional and secure all the time.
- The IDS must be capable of recognizing abnormal traffic and behavior.
- The working of an IDS must not affect the rest of the system's functioning
- The IDS must be adaptive and editable.
- The IDS should detect maximum intrusion with minimum false positive rate.

Terminologies which are covered are as follows:-

- Alert/Alarm: It is a message indicating that a system has been attacked.

- True Positive: An attack is actually encountered which activate the IDS to generate an alarm[17]
- False Positive: Opposite to true positive provoke an IDS to trigger an alert even in case of no intrusive action took place.[17]
- False Negative: It is a severe case if happened where an IDS is unsuccessful to identify an attack[17]
- True Negative :One of the simplest case when there is no intrusions in network no alarm raised[17]

III. ARCHITECTURE OF IDS AND ITS COMPONENTS

An IDS is used to monitor the network traffic which can violate the three principle pillars of security that are Integrity, confidentiality and availability. Integrity refers to ensuring that the source of data is authenticate and there is no alteration in genuine information .Confidentiality means your sensitive information should not be revealed to unauthorized parties. Availability says that data should be available and accessible to only authorized users [22]. Basic architecture of an IDS have some components for intrusion detection are sensors, analyzer, Knowledgebase and User interface. As shown in Fig.1.At first we have collection of dataset in which we do the refining of data in data preprocessing phase, after cleaning of dataset next responsibility is of sensor to analyze the traffic for intrusion detection and also for removal irrelevant data. analyzer next perform its task and if intrusion is recognized ,it will generate alert to adminitrator so that they can take further steps and also knowledgebase is updated with the new attack signatures. Response of IDS can be active or passive. Active means it can terminate the TCP connection itself or block the IP address and in passive response it will simply logs the activity ,send mails to adminitrator, and genrate alarms [21].

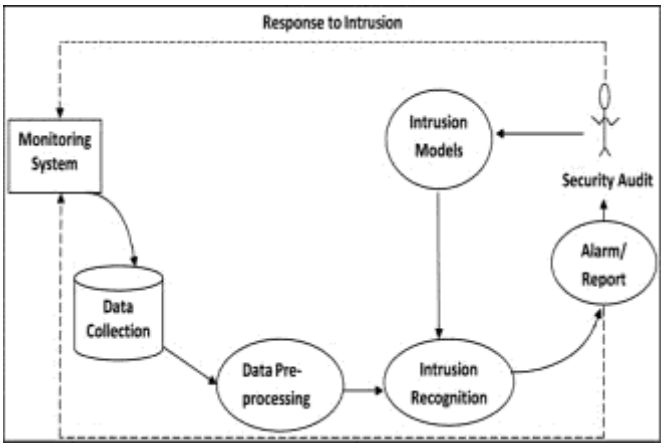

Fig.1. overview of the basic architecture of IDS [16]

In an IDS Architecture we can have some basic components: Sensors or Agents (Host Based), Analyzers, Knowledgebase and User Interface/console.

Sensors/Agents-It is the heart of IDS, Plays vital role in collecting data. They are responsible for sensing the network activity. It performs filtering of information and throw away the irrelevant data and recognizes malicious activity. The term "agent" is mentioned for host-based IDSs.

Analyzer-Role of analyzer is to receive information from the sensors to examine whether an intrusion has been occurred or not.

Knowledgebase-a repository of activity logs for all kind of access and event. Whenever new attacks comes in network update the knowledgebase accordingly so that it can detect variety of attacks.

User Interface/Console- IDS user and system admin where alerts are send uses this interface. Console software is used for laptop, computers.

IV. IDS ATTACKS

A. *Denial-of-Service (DOS) Attacks*

DOS is a kind of service halting attack in which an attacker flood the server system by generating huge amount of service request due to which a legitimate users fails to get the authenticated request's reply. [2].

B. *Eavesdropping Attacks*

It is a kind of sniffing attack. Where a third party tries to steal information from the network if there is any communication gap between sender and receiver.

C. *Spoofing Attacks*

In this attack, hacker pretends to be actual genuine user to access the legitimate information over the internet. There are some common spoofing attacks are as follows IP address spoofing, ARP spoofing, DNS spoofing.[2]

D. *Intrusion attacks or User to Root Attack (U2R)*

An intruder at first enter into a network as normal user and attempts to access the root system via network exploitation. [12].

E. *Logon Abuse Attacks*

This attack wouldn't look for authentication and access privileges, it will simply grant the benefits to an unapproved user [2].

F. *Probing Attack*

It is a kind of attack in which attacker performs scanning for the system which loophole point for a network from vulnerabilities can be encountered like port scanning ,if any port open and connection is not terminated properly terminated can misuse it .some probing attacks are TCP ,

UDP Scanning, SYN, FIN, ACK scanning [12].

V. ANATOMY OF IDS WORKING

The anatomy of IDS consist of mainly four key operations namely, data collection, feature selection, analysis and action, shown in Figure 4.

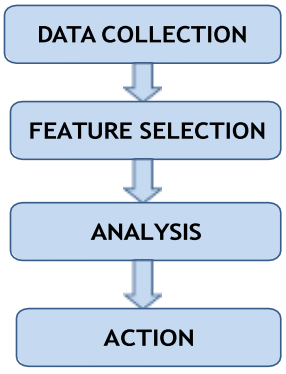

Fig.2. Operation of IDS

A. *Data collection*

At the very first level of IDS implementation we need to do data collection. Data is fed as input to the system. Once data is got collected into a file format then it is further forwarded for analysis. Collection of data is different for both network based IDS and host based IDS. As HIDS is mainly concerned about the data like processing power usage, memory

occupied and disk usage whereas in Network based IDS gather all kind of TCP, IP, ICMP packets with headers and content [13].

B. Feature Selection

Feature selection plays a dominant role in overall enhancement of IDS performance and its accuracy. We come up with a conclusion that by reducing the features to some extent so that we can have only those attributes which are having more intrusive properties rather than considering those which have lower impact on our dataset or less intrusive. This complete process of evaluating only relevant attributes is also famous as feature reduction process. For feature selection we have various techniques like CFS(Correlation Based Feature selection) ,Info gain based, Missing Value Ratio ,Low Variance Filter ,Random forest, backward feature elimination ,PCA(Principle Component Analysis [18].

C. Analysis

Doing analysis is the Key component of IDS working. All the captured network packets or events, log file, access records are analyzed by the IDS by comparing and matching it with predefined rules and signatures [3]. Another method is anomaly based IDS where the system activity is kept on recorded and mathematical models are employed to it which define some rules, it is capable to handling new attack in real time [18].

D. Action

Once any attack recognized by IDS next step is to send alerts to admin either actively or passively. Now it's up to admin how he will take further prevention step, he may drop a particular suspicious packet or terminate a connection [18].

VI. TECHNIQUES USED

IDS follows some techniques to detect an intrusion in a particular network or host. There are two basic techniques used are signature/misuse based and anomaly based. Whenever we are going to install IDS on our network we can buy IDS on the basis of our organization need whether we want signature based detection technique or anomaly based. There are also another dimension available of using these techniques, we may use a multitier architecture of IDS with multiple IDS sensor following distinct techniques to do defense in depth.

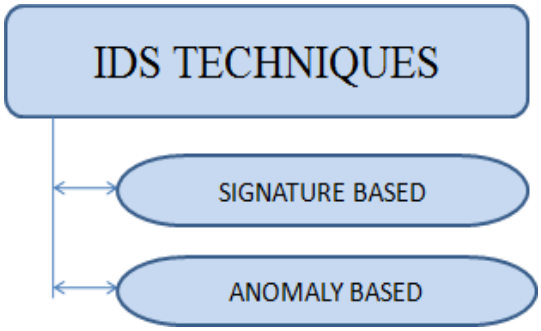

Fig.3.various Intrusion Detection Technique

A. Signature Based IDS

Signature based detection also called as misuse detection, a knowledgebase is prepared before actual working and all the signature, patterns are defined here .if any match found for specific packet from predefined signatures it will generate alerts .it may or may not be capable of identifying many or all attack patterns.

Drawback of this technique is it is not capable enough to identify any new attack or intrusion. It needs signature or software patches to be update all the time. Otherwise it will allow to enter any intrusion into network without any alerts to admin in case of failure of matching patterns for unknown attacks.

B. Anomaly Based IDS

Another useful technique that was implemented to overcome the problems of signature based detection method with novelty is anomaly based detection .this is the active research area, in this method basic or traditional behavior of our

system or network is keep on monitoring if any change or deviation found from actual behavior it report to admin that something suspicious event took place in network. However anomaly based IDS generates high numbers of false positive alarms.[24]

So a lot of research is keep on going on this rule based technique that how can train our IDS in better way to keep this rate lower and make our IDS intelligent enough to differentiate between normal packet and attacks.

VII. TAXONOMY OF INTRUSION DETECTION SYSTEM

On the basis of deployment of IDS it is mainly classified into two types. First is host based another one is network based IDS .IDS can be installed on a specific server or on a host machine as a sensor or agent. Or as whole network monitoring system which is network based IDS deployed before firewall.

A. Host Based IDS

The host based Intrusion detection systems are those on which we installed individual agents on each host machine act as sensor .it performs log analysis, policy violation monitoring, file integrity checking, alerting and active response [23].

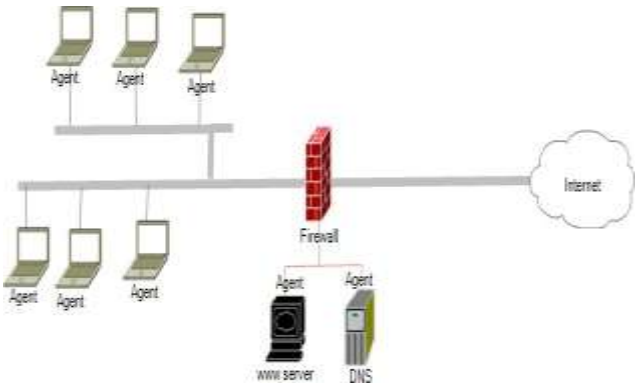

Fig.4.Host Based Intrusion Detection System

1) Advantages of Host based IDS

1. Accreditation of success or failure of an attack: Accuracy of detection of intrusions is higher with lesser false positives than the network based. Host based IDS maintain a complete record of logs consisting of events like who logged in, how many attempts to root login ,password match or mismatch, access time of any credential or any kind of deviation from standardized working all are kept as image in log file. Although response time of network intrusion detection is faster than the other host based and also it do the real time monitoring of packets [11].

2. Monitors System Activities: Host based IDS supremely dedicated to keep eye on overall user and file access activities. It further includes other events like is there any changes to folders of executable file, no of time a root user login or logout in a day ,frequent accesses to a particular file, permission change and accesses etc. [11].

3. Detects attacks that an NIDS can't detect: Some kind of attack which are internal to the network couldn't be notified by the network based IDS .for a scenario there is possibility like an approved user can make changes to system records or file from console window .these kind of attacks can't be captured at networking end [11].

4. No requirement of additional hardware: Host Based IDS work on a single host machine or system or file server, we do not need any extensive hardware or equipment for installation. These sensors are works automatically on the basis of pattern matching or rule based.. Overall deployment expensive are decreased [11].

5. Lower cost: Implementation cost is less as compare to network based IDS but for small networks or with in a network [11].

B. Network Based IDS

The network based IDS is wide in scope, it performs filtering of intrusion for a huge network traffic flowing within in a network through the device. NIDS can also be configured as a tool for sniffing the packets coming from various protocols like TCP/IP, ICMP, IP, and UDP etc. NIDS mainly do prepare the logs of all those activities, events where any deviation found from standard working behavior and forward report to the admin actively through alerts or passively maintaining a record and send a mail to admin [7].

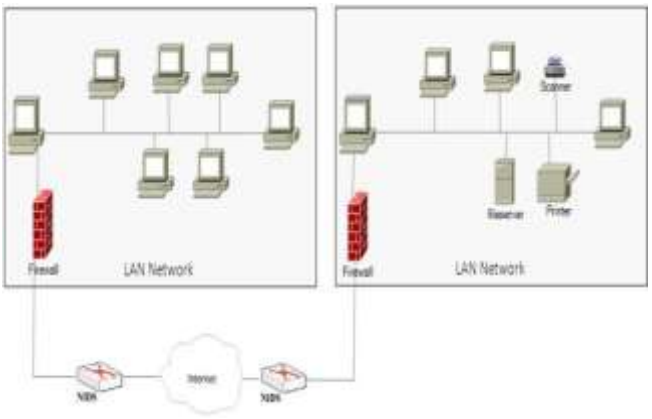

Fig.5.Network Based Intrusion Detection System

Network-based IDS work best when located on the DMZ, on any subnets containing mission critical servers and just inside the firewall. For performing collection of data it does not depends on host based IDS instead of that it is capable of doing self-data collection and from packets which travelling throughout the huge network these network based sensors are stored with predefined rules set and signature and patterns so that if any match found they generate alarm to system admin either in active mode or passive mode. IN case of active mode they will send pop box on screen, or alarms on in case of passive mode they will generate offline mails to admin [10].

VIII. TOOLS IN INTRUSION DETECTION

An intrusion detection product available today addresses a range of organizational security goals [2].This section discusses about the security tools.

A. SNORT

Snort is lightweight and open source software [5]. We can possibly deploy and work any Linux based or Windows based operating systems as it supports many platforms [9].it tracks IP address and keep the various information in documentation format .it automatically generates log files. By performing monitoring of protocol , content searching, Snort detects thousands of worms, viruses, vulnerability exploit attempts ,policy violation, port scans, and other malicious events and activities [9].

B. SURICATA

Also available as third party tool .it is very widely implemented as an alternate option for snort. A very low budget tool which gives great vision throughout the network Offering us a facility to deploy both Suricata and Snort in an hybrid environment

C. FRAGROUTE

Enables us to fragment the IP packets and transformed to the party. Works fine with various platforms and Also known as fragmenting routers.

D. HONEYD

It generates virtual hosts on the network [9]. Provision the flexibility to a host based system to send multiple reuest to multiple address on a LAN .It is possible to knock the virtual machines or to trace route them [9]. Any type of service on the virtual machine can be simulated according to a simple configuration file [9].

IX. ISSUES IN INTRUSION DETECTION SYTEM

A. *False Negatives*

- An IDS actually unsuccessful recognize an intrusion.
- False negatives takes place when an HIDS or NIDS actually not able to capture the intrusion.
- This situation arises if there is any new attack to the network which are previously not defined in knowledgebase.

B. *False Positives*

- Well known as a false alarm.
- When an IDS erroneously identified some "normal" network events as suspicious.
- Administrators should have to keep on updating the new signatures or heuristics whenever comes in existence as soon as possible in order to tackle these unwanted situations.

X. CONCLUSION AND FUTURE WORK

Enabling better security to either organization's internal network most likely to a host based systems or from external whole network based services is an important motivation for IDS migration. These services ensures end-to-end security, overlay on top of virtual networks, span several network segments, and/or cross several layers of networking technologies. From security perspective of network Firewalls are already implemented over there but still there are some kind of patterns and signatures are there for which firewall alone is not capable to tackle. Although firewall protects over network but it need additional security to be added. For providing defense in depth security there is need of Intrusion Detection System implementation [6].

IDS follows a more precise method for signature analysis to recognize the potential attacks but it is also necessary to deploy a robust authentication scenario. As IDS is not a fully automatic attack detection software it needed time to time knowledgebase updating by human assistance or system administrator so that any new signature got identified if came in network. System admin basically keep eye on monitoring the whole network activity.

Hybrid approach of NIDS and HIDS is possible to implement for deploying a more secure IDS but network based IDS is highly recommended for a complete huge network as individually [8]. Installing HIDS may cost more instead of that we can deploy NIDS at center stage. Major problems with NIDS is it produces numerous amount of false positives [20]. Number of research has been done in this direction. Researchers have given feature reduction and classification techniques to reduce this false alarm rate but at still there is possibility like to do multiclass classification for better results and implementations. There are number of classifier like random forest, decision tree c4.5, Clustering, Navies Bayes, also hybrid deployment of algorithm is also possible like c4.5 with SVM (support vector machine), [25]. C4.5 with navies Bayes etc. Target is to reduce false alarm rates for better accuracy and performance.

X. REFERENCES

1. J. P. Anderson, "Computer Security Threat monitoring and surveillance", *Technical report*, JP Anderson Co., Apr 1980.
2. . Karthikeyan .K.R and A. Indra- "Intrusion Detection Tools and Techniques a Survey"
3. Sriram Sundar Rajan, Vijaya Krishna Cherukuri-"An Overview of Intrusion Detection Systems".
4. John McHugh, Alan Christie, and Julia Allen- "The Role of Intrusion Detection Systems"- Software Engineering Institute, CERT Coordination Center
5. Snort: The open source network intrusion detection system.
6. P. Uppuluri, R. Sekar, "Experiences with Specification-Based Intrusion Detection System", *Recent Advances in Intrusion Detection: 4th International Symposium RAID 2001*, pp. 172, October 10–12, 2001.
7. VernPaxson, "Bro: a system for detecting network intruders in real-time" in Computer Networks, Amsterdam, Netherlands:Paxson, vol. 31, no. 23–24, pp. 2435-2463, 1999.
8. David J. Day, Denys A. Flores, Harjinder Singh Lallie, "CONDOR: A Hybrid IDS to Offer Improved Intrusion Detection", *Trust Security and Privacy in Computing and Communications (TrustCom) 2012 IEEE 11th International Conference on*, pp. 931-936, 2012.
9. "Top 125 Network Security Tools"- SecTools.Org- http://sectools.org/tag/ids/sec .

10. "Global Information Assurance Certification Paper"- Copyright SANS Institute Copyright SANS Institute Author Retains Full Rights
11. "SANS penetration testing copyright by SANS"-Copyright SANS Institute Author Retains Full Rights.
12. Swati Paliwal ,Ravindra Gupta Assistant Professor "Denial-of- Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 60– No.19, December 2012
13. Dr. S.Vijayarani1 and Ms. Maria Sylviaa.S," INTRUSION DETECTION SYSTEM – A STUDY " International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015
14. Paul Innella- "The Evolution of Intrusion Detection Systems"- Tetrad Digital Integrity, LLC. International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015
15. Christopher Low –"Understanding Wireless attacks &detection "-GIAC Security Essentials Certification (GSEC) Practical Assignment 13 April 2005 - SANS Institute InfoSec Reading Room.
16. 6 G.V.NadiammaiM.Hemalatha-" Effective approach toward Intrusion Detection System using data mining techniques"Egyptian Informatics Journal Volume 15, Issue 1, March 2014.
17. Ms. Urvashi Modi Prof. Anurag "A survey of IDS classification using KDD CUP 99 dataset in WEKA" International Journal of Scientific & Engineering Research, Volume 6, Issue 11, November-2015.
18. . International Journal of Computing and Business Research (IJCBR)ISSN:2229-6166 vol. 4 Issue 2 May 2013,"Intrusion Detection System and Intrusion Prevention System :A Comparative Study
19. 1Jayesh Surana,."A Survey On Intrusion Detection System" International Journal of Engineering Development and Research (www.ijedr.org), © 2017 IJEDR | Volume 5, Issue 2 | ISSN: 2321-9939
20. MOHAMMED HASAN ALI 1, BAHAA ABBAS DAWOOD AL MOHAMMED 2, ALYANI ISMAIL2, (Member, IEEE), AND MOHAMAD FADLI ZOLKIPLI1 1Faculty of Computer Systems and Software Engineering, University Malaysia Pahang, Malaysia 26300." A New Intrusion Detection System Based on Fast Learning Network and Particle Swarm Optimization" [accessed Oct 26 2018].
21. Asmaa Shaker Ashoor, Prof. Sharad Gore – "Importance of Intrusion Detection System"-International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011.
22. Jayesh Surana,,"A Survey On Intrusion Detection System" International Journal of Engineering Development and Research (www.ijedr.org), © 2017 IJEDR | Volume 5, Issue 2 | ISSN: 2321-9939
23. Steven R. Snapp, James Brento,"DIDS(Distributed Intrusion Detection System)- Motivation, Archictecture and An Early Prototype", June, 2008.
24. Sharmila kishor wagh,"Survey on Intrusion Detection System Using Machine Learning Techniques", Sep, 13.
25. Vaisalikosamkar,"An Improved Intrusion detection system using c4.5 decision tree and support vector machine", IJCSIT 2014.