General Study of Intrusion Detection System and Survey of Agent Based Intrusion Detection System

[1]Aumreesh Ku. Saxena
PhD Scholar, CSE Dept. AISECT
Bhopal, India
Aumreesh@gmail.com

[2]Dr. Sitesh Sinha
Prof. CSE Dept. AISECT
Bhopal, India
siteshkumarsinha@gmail.com

[3]Dr. Piyush Shukla
Prof. CSE Dept. UIT RGPV
Bhopal, India
pphdwss@gmail.com

Abstract—**In today's world one of the most severe threat to computer security is the illegal intrusion into a computer system. As the network applications are growing rapidly, new sort of network attacks are rising continuously. The intrusion detection system IDS is used for the detection of the intrusion activity extends over the public network. IDS may need to deal with different audit record format. IDS have turn out to be essential security tool for detecting the attacks on computer network and resources. Due to this, we presented a review (general study) on IDS. First, we will discuss about intrusion detection later will discuss the type of IDS. We have emphasize on the range of type of IDS like anomaly, misuse, host based, network based and hybrid IDS, specifically IDS based on the anomaly or behavior based IDS along with Agent based technology in real network. At last, the contribution of every single type of IDS is described.**

Keywords— Intrusion, Anomaly, Network, IDS, Host, Misuse, Agent, Mobile Agent

I. INTRODUCTION

A propel insurance approach is normal thief caution that numerous organizations of vast scale and little scale used to shield their foundation from burglary. Giving the idea of this framework is to provide staggering certainty for various organizations which can introduce any sort of security to secure systems against robbery or assault [1]. **Intrusion Detection System (IDS)** is a fundamental arrangement of thief caution for system. It empowers the checking of the system from a meddling activity [1].

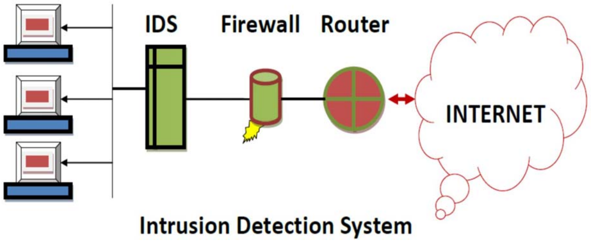

Fig. 1. Intrusion Detection System

On the off chance that a meddling activity has discovered, and then IDS see Fig 1 can create an alert to advice about the assault on system [2]. Like the standard thing criminal alerts, in any case, IDS can produce false-cautions or false-positives [3, 4]. The false-positive may found if IDS can produce a caution against the typical activity of the client. At the point when the IDS create a few false-positives, then it can diminish trust in the IDS capacity to secure the system [4, 5]. Thus, it is hard to build up IDS to drop down the era of false-positives [4]. The IDS can likewise confront the false-negatives. In this situation, assault has happened against the system and IDS may neglect to produce the caution regardless of the possibility that it is built up to distinguish these assault. IDS ought to never produce the false-negatives. Or maybe, it is decided on IDS to deliver some false-positives than to produce any of the other false-negatives [5, 6]. In the present scenario where most of the people are going toward digitalization, so security of data is prim concerned. Hence an idea needs to improve existing IDS mechanism which allows security of the systems over network and free from the malicious user attacks. With this approach we have study various types of IDS which is describe in section 2. Section 3 is showing related work, in this various existing agent based IDS discussed. Section 4 is the conclusion.

II. TYPE OF IDS

To secure system, IDS must create an alert as though it identifies a meddling activity over the system. A few IDSs can enact the cautions in light of many sort of exercises on system. The two normal methodologies of initiating are clarified here [11]:

- Misuse recognition and
- Anomaly recognition

Or maybe initiating strategy, IDS must break down for meddling activity at the particular focus over the system. Controlling meddling activities happens at given two ranges [11]:

- Network-based and
- Host-based

In last, a few interruption discovery frameworks consolidate with many elements in a solitary framework. These sorts of frameworks are named as half and half frameworks.

ISBN: 978-1-5090-6471-7/17/$31.00 ©2017 IEEE

A. Anomaly Recognization

Alongside the recognition method is to deliver a profile for every gathering of the clients in framework. These profiles can be produced consequently or physically both. Gradual instructions to make these profiles are not essential if these profiles are displaying the elements precisely for every gathering of the client over the system. These sort of profiles are used as the benchmark to show ordinary client's activity. In an event that any action of the system may contrast from this given gauge, then the movement may deliver a caution [14, 16].

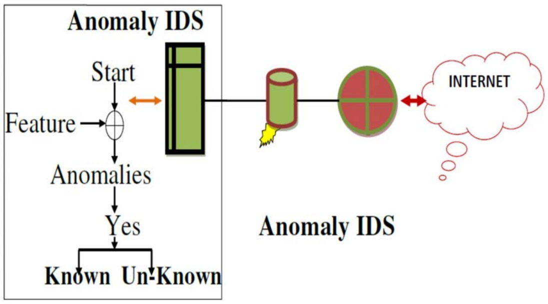

Fig. 2. Anomaly IDS

As this sort of IDS is built up encompassing profiles of the client, consequently it is additionally named as profile-based-identification see Fig 2.

Advantages: The inconsistency recognition frameworks may give few benefits. Towards the starting, anomaly IDS can recognize insider-assaults or record burglary effortlessly. On the off chance that, genuine client or any other person is expending the stolen-account, begins doing the activities that are outer to the ordinary profile of the client, it then delivers a caution. After that, since framework depends on redid profiles, along these lines it is troublesome for assailant to acknowledge with affirmation, what activity can be stolen out without setting-away caution. Evidently significant advantage of meddling activity is not in view of particular kind of movement that displays the notable meddling activity as inside the mark subordinate IDS [14, 16]. The uneven location framework can essentially recognize an assault. The meddling activity produced an alert as soon as it vary from an ordinary activity, and are not a result of another person which can designed the framework to examine the particular movement stream [16].

Disadvantages: As each IDS uneven location frameworks additionally endures few negative marks. The underlying clear fault is that the framework must be prepared to make appropriate profiles of the client. At the time of preparation of profile to clarify what the standard activity appears as on the system, which is not secured against the assault. Profiles maintenance may likewise be extremely tedious [6]. Albeit, real bad mark for inconsistency identification is the multifaceted nature of the framework and trouble of partner a caution with certain occasion that set off the alert. Moreover, there is no certification that they may have that particular assault can even deliver the caution. In the event that the meddling activity is close to ordinary activity of client, after that, assault will be available. It is additionally confounded to comprehend the kind of assault that might be set-off the alerts aside from the assaults against system through utilizing a few profiles of client [6].

B. Misuse Recognisation

Another real classification of IDS-activating is alluding as misuse recognition. The misuse recognition in Fig 3 is likewise alluded as the mark based-identification consider figure to be alerts are delivered in view of certain assault marks [1, 2, 3].

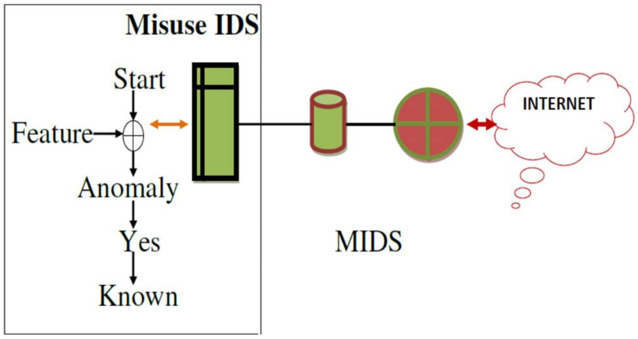

Fig. 3. Misuse IDS

These assault marks comprise of particular activity or movement that depends on known meddling activity.

Advantages: The misuse discovery permits many advantages. One of them is the mark definitions which are created on known meddling activity. Furthermore, the client can manage the mark database, and investigate that misuse recognition framework is customized for meddling action [1]. Last legitimacy is that the framework is effectively learned. On the off chance the client can relate specifically to certain sort of activity over the system [2].

Disadvantages: Along with a few benefits, misuse recognition frameworks can have a few negative marks. A fundamental issue is dealing with the condition of-data for marks in which a meddling activity incorporates numerous discrete-occasions in which, entire assault signature may found inside more than one bundle over the system. Other negative mark of this misuse identification framework must have signature display over entire clear assaults that the assailant may deliver against the system [6]. Furthermore, last and primary issue alongside misuse identification frameworks is that abuse recognition framework may get set-up by anybody in the lab and can intentionally attempt to discover the approaches to start the assault which keeps away from the location by abuse discovery framework [6].

C. Location Based IDS

To decide the movement of system and activate the caution as when the system is under the assault, the IDS ought to screen the system at the specific focus. Two common checking spots are said as beneath:

a) Host-based and
b) Network-based

a) Host Based IDS

Host-based IDS Fig 4 shows the checking of framework which looks for data at nearby host or the working framework. This might be accomplished by a confounded framework which decides the correct framework call or it might be straightforward, for example, essentially inspecting framework log documents [8, 9].

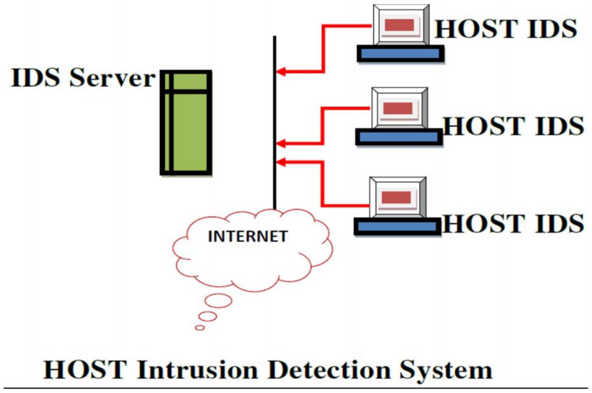

Fig. 4. HOST IDS

Few of these methodologies may precisely hold the assaults before they may succeed, while the others just provide details regarding what has happened already.

Advantages: The main advantage of the host-based observing framework is the accomplishment of assault which can be analyzed. The system subordinate framework can create caution on the nearness of any prominent action; however they can't generally affirm the achievement or disappointment of these assaults [8, 9]. One of the last values of the host-based-checking framework is, if arranged activity stream gets scrambled, then host-based-observing framework has the entrance of movement in a decoded shape.

Disadvantages: Two noteworthy downsides to a host-based-checking framework are specified as: Incomplete system picture and Necessity to bolster numerous working frameworks. By just deciding the data at level of neighborhood host, the host-base-checking framework has the complexity in building the precise picture of system or coordinating the occasions happening crosswise over whole system [6, 9]. The other trouble lies in actuality that the host-based-observing framework needs to keep running on each framework on the system. This requires confirmation of backing for whole extraordinary working frameworks.

b) Network Based IDS

Set up of looking for unobtrusive movement at host-level, the system based-monitoring systems decide the correct bundles of nodes which are going around the system. The framework decides this movement for the known images of the informative action. Since these frameworks are watching node movement, any assault marks identified may succeed or come up short. It is typically troublesome, if not inconceivable for the system based-observing frameworks to serve the disappointment or correct assaults [9, 14]. Fig 5 is showing network intrusion detection system.

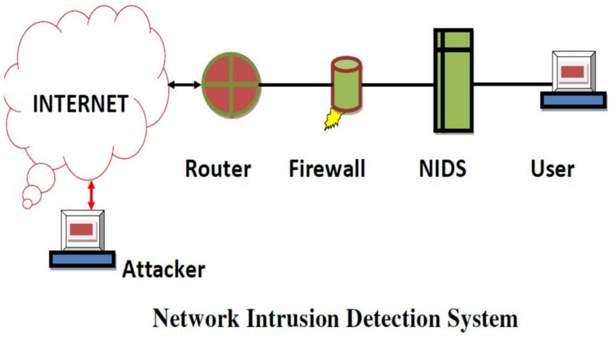

Fig. 5. NIDS

Advantages: A system based observing framework has preferred standpoint of organizing and seeing the assaults which are establishing around the entire system effortlessly. Seeing assaults against the whole arrangement, gives a perfect sign of range to which the system get attacked [9]. Furthermore, as a proof, the checking framework is the main analyzing movement of the system for every sort of the working framework which is used on system [9].

Disadvantages: Encryption of the activity stream of system may fundamentally be based on IDS. Potentially the significant drawback is arrange based-checking, however, the systems has turned out to be quickly bigger alongside regard to the data transmission, it has turns out to be more hard to place organized IDS at a solitary area on system and catch the whole movement effectively. This then requires the employments of the more sensors all through system, which expands the expenses of IDS [7, 6].

III. Related Work

Snort is a open-source IDS tools which is used for detecting as well as preventing attacks, for example, as soon as attacks are identified, the connection can be chunked instantly to stop entering any malicious and attacks to the network system. In hybrid approach which is the combination of Snort and PHAD (Payload Hybrid Anomaly Detection) detects both types of attacks which are anomaly based and misuse based [2, 3]. A flow-based feature generation and automatic rule-generation intrusion detection systems are selecting 17 features from network packet and their combination in order to generate rules. The main application of these IDS is automatic updates [4]. Online Sequential Extreme Learning Machine (OS-ELM) based IDS with network traffic profiling is tested on specific Data Set known as alpha- FST-Beta IDS [7]. The training connections are first categorized on the basis of protocol and service features. This categorization is named as alpha profiling [7]. It increases the scalability and reduces the time complexity of IDS. Large feature set of network traffic dataset is reduced using ensemble of three feature selection techniques [7]. Beta profiling is used to reduce the size of training dataset [7]. The combination of MAS (Multi agents Systems) and CBR (Case Based Reasoning) technique are producing architecture of intelligent intrusion detection based on multi-agent systems which presents a distribution of sensing activities and effective interoperation between agents [9]. It is important to note that in contrast to a monolithic system proposed model has better scalability [9]. Another IDS based on Grid computing which is concentrating on flexibility and interoperability of mobile agents, integrated with cryptographic traces technique based on chaining mechanism to conserve a proof of jobs execution. This Grid based IDS are producing well results in terms of low response time, less network load and high intrusion detection capacity [10].

A comparative analysis of various mobile agent techniques are presented in [12] on the basis of analysis we have observed that Packet dropping is one cause of high false alarm rate. BPNN (Back-Propagation Neural Networks) technique reduces detection time and false alarm rate Where ANN (Artificial Neural Network) based technique can be used to reduce the size of payload [12]. If we want to improve response time in mobile agent based IDS then use client – server architecture [12]. Another Mobile Agent based technology presented for distributed systems with the feature of mobility, independence, Dynamic Adaptation, Accessibility, Scalability system [13]. Another distributed mobile agents IDS architecture named DIDMAS is presented in [15]. DIDMAS distributed the task associated to every intrusion, reducing the work load done by individual node and removing an individual node bottleneck [15]. Distributed detection takes place long time in integration of data where DIDMAS can migrate to detection place and analyzes data locally which considerably decrease the detection delay [15]. DIDMAS deployed new rules and action without any change in existing gents set [15]. Another IDS architecture named Laocoonte is presented, which focused on internal security and to minimize assault. Due to hierarchical system of Laocoonte it has several levels to execute event correlation, also perform controlling through central nodes. Cooperative agents are used to appeal a simple mathematical action and verified results [17]. Another multi-agent based IDS called MAJIDS (multi-agent based intelligent intrusion detection system) are presented in [18] this learning agent module can self-adjusting learn network data and host data using data mining approaches, like the association rules and artificial neural network, and so on [18]. Rules are producing through the learning agent, and through detection agent, detect data as per rules and reply to them. Through multi agent, error can be reduced during learning process. Another important factor with multi agent is that if one agent not succeeded to learn data, the other agents can take over [18].

IV. Conclusion

We have discussed different types of intrusion detection systems based on agent based technology for anomaly IDS to improve detection rate like false positive rate, reduce false negative rate, and security that can be worked on various platforms. There have incredible IDS research to deploy an agent based IDS for security, which means an agent move in the network called mobile agent to capture packet and detect anomalies. Further we have identified that Grid computing is very useful for IDS with this technique we can increase the flexibility and interoperability of mobile agents. We have also observed that combination of MAS (Multi agents Systems) and CBR (Case Based Reasoning) technique are providing effective communication between agents and producing better scalability. To implement IDS and test anomalies we have various tools like snort, Security Onion, OSSEC, OpenWIPS-NG, Suricata, Bro IDS and many more. However, the accuracy and security issues are not decisive and still in its infancy. Another solution, taking into consideration of various factors and scheme, may be expanded to deal with accuracy and security issues. BPNN (Back-Propagation Neural Networks) technique and ANN (Artificial Neural Network) based technique can also be helpful in IDS to reduce response time and payload. Mobile agent-based technique in distributed system, realizes the scalability and it can reduce the response time as well as bandwidth consumption. Intelligent multi-agent based intrusion detection system can be self adapting, learner and rules generated. And last from the survey of several agent based IDS we have listed some advantages of agents in IDS

- Independent Execution
- Platform Autonomy
- Dynamic Adaptation
- Accessibility
- Scalability
- Network Latency Trounce
- Network Load Decrease

References

[1] Akash Garg; Prachi Maheshwari “A hybrid intrusion detection system: A review” 2016 10th International Conference on Intelligent Systems and Control (ISCO) Year: 2016 Pages: 1 - 5,

[2] Akash Garg; Prachi Maheshwari “Identifying anomalies in network traffic using hybrid Intrusion DetectionSystem” 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS) Year: 2016, Volume: 01 Pages: 1 - 6,

[3] Akash Garg; Prachi Maheshwari “Performance analysis of Snort-based Intrusion Detection System” 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS) Year: 2016, Volume: 01 Pages: 1 – 5

[4] Naser Fallahi; Ashkan Sami; Morteza Tajbakhsh “ Automated flow-based rule generation for network intrusion detectionsystems” 2016 24th

Iranian Conference on Electrical Engineering (ICEE) Year: 2016 Pages: 1948 - 1953,

[5] Audrey A. Gendreau; Michael Moorman " Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things" 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud) Year: 2016 Pages: 84 - 90,

[6] Farid Lawan Bello; Kiran Ravulakollu; Amrita "Analysis and evaluation of hybrid intrusion detection system models" 2015 International Conference on Computers, Communications, and Systems(ICCCS) Year: 2015 Pages: 93 - 97,

[7] Raman Singh; Harish Kumar; R. K. Singla " Performance analysis of an Intrusion Detection System using Panjab University Intrusion Data Set" 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS) Year: 2015 Pages: 1 - 6,

[8] Agustinus Jacobus; Alicia A. E. Sinsuw "Network packet data online processing for intrusion detection system" 2015 1st International Conference on Wireless and Telematics (ICWT) Year: 2015 Pages: 1 - 4,

[9] Mohssine El Ajjouri; Siham Benhadou; Hicham Medromi "New collaborative intrusion detection architecture based on multi agent systems" 2015 International Conference on Wireless Networks and Mobile Communications (WINCOM) Year: 2015 Pages: 1 - 6,

[10] Mohammed Ennahbaoui; Hind Idrissi; Said El Hajji "Secure and flexible grid computing based intrusion detection system using mobile agents and cryptographic traces" 2015 11th International Conference on Innovations in Information Technology (IIT) Year: 2015 Pages: 314 - 319,

[11] Loubna Dali; Ahmed Bentajer; Elmoutaoukkil Abdelmajid; Karim Abouelmehdi; Hoda Elsayed; Eladnani Fatiha; Benihssane Abderahim "A survey of intrusion detection system" 2015 2nd World Symposium on Web Applications and Networking (WSWAN) Year: 2015 Pages: 1 - 6,

[12] Bhavin Shah; Bhushan H. Trivedi " Improving Performance of Mobile Agent Based Intrusion Detection System" 2015 Fifth International Conference on Advanced Computing & Communication Technologies Year: 2015 Pages: 425 - 430,

[13] Okan Can "Mobile agent based intrusion detection system" 22nd Signal Processing and Communications Applications Conference (SIU) Year: 2014 Pages: 1363 - 1366,

[14] A. Kartit, A. Saidi, F. Bezzazi, M. El Marraki & A. Radi, "A new approach to intrusion detection system", Journal of Theoretical and Applied Information Technology, Vol. 36, No. 2, 2012, pp. 284-289

[15] Imen Brahmi; Sadok Ben Yahia; Pascal Poncelet " A SNORT-based Mobile Agent for a Distributed Intrusion Detection System" Proceedings of the International Conference on Security and Cryptography Year: 2011Pages: 198 - 207

[16] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez,``Anomaly-based network intrusion detection: Techniques, systems and challenges," Comput. Secur., vol. 28, nos. 1_2, pp. 18_28, 2009.

[17] Rafael Paez; Miguel Torres " Laocoonte: An agent based Intrusion Detection System" 2009 International Symposium on Collaborative Technologies and Systems Year: 2009 Pages: 217 - 224,

[18] Xiaodong Zhu; Zhiqiu Huang; Hang Zhou "Design of a Multi-agent Based Intelligent Intrusion Detection System" 2006 First International Symposium on Pervasive Computing and Applications Year: 2006 Pages: 290 - 295,