A Review on Intrusion Detection System for Networks

[1]Haritha S Kumar, [2]Nitesh Kumar, [3]Manjula Devi T H

[1]Student of M.Tech, [2]Scientist/Engineer –'E', [3]Sr. Assistant Professor

[1,3]Department of TCE, [2]ISTRAC

[1,3]DSCE, Bengaluru, [2]ISRO

***Abstract*: Computer and mobile networks have become an unavoidable entity in everybody's daily life, from online shopping to banking, news to entertainment, etc it provides everything. Ensuring a safe network is every network engineer's tedious task. Having a huge amount of data to play with hackers and intruders are always trying to attack the network. It's as difficult as to maintain the network safely as it is to build one. There are many types of attacks and their prevention and protection available in the current trend, yet there is also an increase in the new type of attacks day by day. The review paper aims to give a brief idea of what's a network and its related security issues especially about passive attacks and how to detect and prevent them, by using the existing methods and tools available.**

***Keywords*: Networks, Network Attacks, Passive Attacks, Intrusion Detection System (IDS), Open Source Tools for IDS, Advantages and Disadvantages of IDS.**

I. INTRODUCTION

A connection between two or more electronic equipment's for sharing of information and resources can be termed as a network. The network can be wired or wireless. There are various parameters that keep a network strong, few of them are, data transfer speed, memory, cost, etc. Just as technology continues to improve, devices are more improving towards mobile and wireless connectivity. This new era of technological usage can also provide a risk of network security threats not only in the work environment but also to the privacy of users at home. Our ability to remain equally as informed and vigilant as newer technology emerge may have a huge effect on how we design the plan for network protection approach and against unauthorized intrusions of the future [1].Network attacks on power system through an information communication system may lead to damage to important equipment, causing a major blackout accident and problems, which may even lead to other infrastructure systems paralyzed making it less efficient [2]. There are mainly two types of security attacks which are passive attack where the intruder allows something to happen in the network without reacting or trying to stop it by just watching, noticing, or making a statement from the information within it, the user may not be aware of the passive attack in most of the cases. On the other hand, active attacks consist of disturbing/annoying or altering the user network to get the behavior and/or results from its which is used to discover secret data within it for certain intentions, the user may lose the data. Few examples of attacks are Traffic Jamming, Malicious Behaviors of nodes, DOS, Traffic Analysis, Eavesdropping, Session hijacking, SYN flooding, and so on.

II. PASSIVE ATTACKS

The hardest part of network security is to protect the traffic content of it from passive attack. During transmission of data there is a high threat on data as many intruders are waiting to get a chance to attack the data.it has been figured out that the complexly structured internet can hide the possible risk to the user of the computer especially about passive attack, hence it is always undetectable and unpredictable and also have dynamic and ever-changing behavior, Due to the high mobility and wireless medium, third party can easily access the data and make the disturbances to the source and destination[3].Hence passive attack is one where the attackers get all the information that is required without any knowledge of the user of the network, which can be mentioned as eavesdropping. There are different types of passive attack, few of them are timing attack where the attacker carefully observers the time taken for a data transmitted between two parties and gets some inferences from it [4]. Traffic analysis where the packets sent through the traffic and also the amount of traffic in the network is monitored by the intruder and further conclusions are made [5]. The efficient way to keep the network safe is to prevent it from any type of attacks from unauthorized and vulnerable sources.

III INTRUSION DETECTION SYSTEM

Intrusion detection is a process of watching or supervising the events happening in a computer system or network which helps in finding the existence of any possible threats or attacks. The intrusion detection system (IDS) is a mechanism used for intrusion detection which has some set of policies and rules that are followed. IDS help in maintaining a healthy and safe network by providing data integrity, confidentiality etc [6]. Typically, an IDS is connected to security information and event management (SIEM) system, which collects outputs from various security systems and filters out malicious activities from false alarms and reports them. The two types of IDS are host-based intrusion detection (HIDS) and network-based intrusion detection (nibs). HIDS works on a particular device within a network, it is used to collect and monitor the inbound and outbound traffic with respect to that particular system [7]. It then analyzes the traffic and detects if any suspicious activity has occurred or not. The can thoroughly inspect all the aspects of the device including system file modification, user authentications etc. NIDS is installed on a specific point on a network independent of the operating systems so that it can monitor all the devices present in the network, where it monitors incoming and outgoing traffic at a network level and finds conclusions about the safety of it [8]. NIDS can be online or offline, where online NIDS provides real-time security at high rates, and offline NIDS works on the stored data within the network systems.

IV METHODS IN IDS

The two main methods available for IDS is signature based IDS and anomaly-based IDS [9]. The signature-based IDS act on the packets generated by the traffic and compared it with the already existing signatures in the stored database of the IDS. The database consists of all the available set of attacks or suspicious activity which was occurred in the system previously if any of the signature matches then an alert is generated about it [10]. The advantage of signature-based IDS is that it does not need to create a new pattern for attack every time since it has already stored the attack pattern in the database which makes it easier for comparing and detecting the same type of attack if it occurs in future. It already knows the vulnerability and can provide sufficient security alerts even before the attack is successful. The disadvantage of this is it cannot detect any new pattern in real time quickly. The database must be updated often for proper security. The anomaly-based IDS [11] is a detection method where the software monitors the normal system pattern in real time and any deviation in it, an alert is initiated. It provides a fast response if anything other than normal behavior is observed. To implement anomaly-based IDS, two phases are used: Training phase and the testing phase. In the training phase, the normal behavior of the system is observed in the absence of malicious activity. Based on these observations, a profile is built. In the testing phase, the current behavior of the system is compared with the stored profile and any deviation from the stored profile is considered an attack on the system. The problem with anomaly-based IDS is that it generates a large number of false alarms if anything new is detected irrespective of whether it is an actual attack or a genuine work it gives an alert.

V IDS FUNCTIONS

The IDS works in the following manner, it has four main steps [12]

1. Data acquisition: the data generated by the system in the form of logs are is collected and converted into the desired format for processing. Network-based IDS collects and alters the data packets and in host-based IDS collects details like usage of the disk and processes of a system.

2. Selection of features: from the vast set of data collected only the desired set of details have to be filtered to detect the treat. For example, the Internet Protocol (IP) address of the source and destination system, protocol type, header length, and size could be taken as a key for intrusion selection.

3. Data analysis: the filtered data must be thoroughly analyzed to detect threats or attacks. Signature based IDS analyze the data where the incoming traffic is checked against a predefined signature or pattern. Another method is anomaly based IDS where the system behavior is studied and mathematical models are employed to it.

4. Action: this refers to how the system reacts to the threat if anything is detected after analysis, it can provide an alarm or email alert to the system administrator, or else it can drop or block the unwanted packets depending on the rules written for it.

VI TOOLS FOR IDS

There are many IDS tools as open source available presently for all type of operating systems, few of them which are popular are as follows [13].

1. **Snort -** Snort is a lightweight software which is developed in 1998 by Mart. It basically acts a packet sniffer, logger or as a network level detection and prevention system. It will read the packets and display them onto the console which it supports. Detection is based on the rules provided by the user. Pros include easy installation and run, user-customized rules, available for both Windows and Linux. Cons are it has less packet capturing and GUI, it supports only medium level for high-speed network

2. **Suricata -** Suricata is a quick and robust network intrusion detection system. It is both on signature-based and anomaly-based approach. It uses Lua which is a very powerful scripting language. It has advanced filters for alerts. Advantages are it has advanced featured like multi-reading capabilities and GPU acceleration, and reusability. Disadvantages are it generates more false alarms and also uses the resources of system and network at a high rate.

3. **Bro IDS-**Bro IDS is an anomaly-based approach, and is usually combined with Snort for better performance, Bro IDS uses a domain specific language for networking named as Bro. This is broadly used in forensics and other such related cases. The policies used here detects the suspicious or unmatched packets. It is a script-driven IDS. Advantages are it can support high throughput environments and has very less processing time. The drawback of this that the user needs to be more careful and versatile while specifying the rules since it is a script-driven IDS, it is also complicated to write down policies.

4. **OSSEC**- OSSEC is a Host-based IDS. It is a multi-platform, scalable, and open source tool. It fundamentally only stores alert but not all the logs. It has a powerful correlation and analysis engine, file integrity checking, integrating log analysis facility; centralized policy enforcement real-time alerting and active response. This is capable of detection DOS attack. Pros are the storage overhead is reduced. And it is easy to install and customize, also it supports multi-platforms. Cons include a transition to a newer version of the platform is tedious and the up gradation overwrites all the existing rules, in some cases, the user-customized rules may get deleted

5. **Security Onion** - Security onion is an Ubuntu-based Linux distribution tool for IDS and network security monitoring (NSM), WITH THE Functionalities such as full packet capturing process, NIDS and HIDS. The merits include it provides multiple IDS options, gives log and alert data for events detected within the system. Demerits are these are a highly specialized purpose, not all Linux distributions have them in their repositories. And their installation from the source code may be difficult.

VII ADVANTAGES OF THE IDS

1. Monitors the system both internally and externally for any malicious activity [14]
2. The user can customize the filters according to the level of security needed [14].
3. It is fast and efficient even in monitoring the real-time data from the network [15].
4. There are many open source tools available for IDS which helps in cost-effective security management[15]
5. Can be used in wide range of application such as machine learning, artificial intelligence, iot, mobile networks, and so on...[18][19].

VII DISADVANTAGES OF THE IDS

1. Creates a large number of false alerts [16].
2. Only the alert is being given by the system, the protection must be done manually [16]
3. The coding for the open source tools is quite difficult because of fewer documentations available [16].
4. The only signature-based or anomaly based doesn't provide a complete solution, hence there is a need for a hybrid type of IDS[17]
5. At times updating of the system may lead to loss of the IDS data, which may have crucial information [20].

IX CONCLUSION

This paper gives a review about network and its security related issues, especially on passive attacks. The passive attacks are detected by an intrusion detection system, which gives alert on any unusual event happening the network. Various features of IDS is mentioned, the open source tools which can be used for configuring IDS for efficient monitoring of the system is given along with its advantages and disadvantages . Thus one can be sure of the features and tools available for IDS in the present internet world.

REFERENCES

[1] Alireza Kavianpour, Ph.D. Michael C Anderson, BSEET, "An Overview of Wireless Network Security", 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing, PP 306-309

[2] Biyun Chen, Qiaoling Dai, Zhiwei Cui, "Risk Assessment of Distribution Network Considering Network Attack", 978-1-5386-1427-3/17/$31.00, 2017 IEEE, PP 1-4

[3] J.Vijitha Ananthi, S.Vengatesan "Detection of Various Attacks in Wireless Adhoc Networks and Its Performance Analysis", Proceedings of the International Conference on Inventive Computing and Informatics (ICICI 2017) IEEE Xplore Compliant - Part Number: CFP17L34-ART, ISBN: 978-1-5386-4031-9, PP 754-757

[4] Rahma MEDDEB, Bayrem TRIKI, Farah JEMILI and Ouajdi KORBAA, "A survey of Attacks in Mobile Ad hoc Networks", 978-1-5090-6778-7/17/$31.00 ©2017 IEEE, PP 1-7

[5] Alejandra Guadalupe Silva Trujillo1· Ana Lucila Sandoval Orozco2· Luis Javier Garc´ıa Villalba2·Tai-Hoon Kim3 "A traffic analysis attack to compute social network measures", Multimedia Tools Appl https://doi.org/10.1007/s11042-018-6217-9, JUNE -2018, PP 1-15

[6] Rafath Samrin, D Vasumathi "Review on Anomaly-based Network Intrusion Detection System" 2017 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), PP 1-7

[7] Arsalan Ali Shaikh, Heng Qi, Wei Jiang, Muhammad Tahir, "A Novel HIDS and Log Collection Based System for Digital Forensics in Cloud Environment", 2017 3rd IEEE International Conference on Computer and Communications, PP 1434-1438

[8] Cheng-Hung Lin and Cheng-Hung Hsieh," A Novel Hierarchical Parallelism for Accelerating NIDS Using GPUs", Proceedings of IEEE International Conference on Applied System Innovation 2018, PP 578-581

[9] Arkadiusz Warzyński and Grzegorz Kołaczek,“ Intrusion detection systems vulnerability on adversarial examples", 978-1-5386-5150 6/18/$31.00©2018 European Union, PP 1-4

[10] Abdullah H Almutairi, Dr. Nabih T Abdelmajeed, "Innovative Signature-Based Intrusion Detection System", 11. Saba Khan Prof. Dilip Motwani," Implementation of IDS for Web Application Attack using Evolutionary Algorithm", 978-1-5386-3148-5/17/$31.00 © 2017 IEEE, PP 114-119

[11] Saba Khan, Prof. Dilip Motwani," Implementation of IDS for Web Application Attack using Evolutionary Algorithm", 2017 International Conference on Intelligent Computing and Control (I2C2), PP 1-5

[12] Mohit Tiwari, Raj Kumar, Akash Bharti, Jai Kishan "Intrusion Detection System", International Journal of Technical Research and Applications · April 2017, 38-44

[13] Resmi A M, Dr. R Manicka chezian, "Intrusion Detection System Techniques and Tools: A Survey", Sch. J. Eng. Tech., 2017; 5(3): PP 122-130

[14] Dr C Manju "Performance Evaluation of Intrusion Detection System Using Classification Algorithms", DOI:10.15680/IJIRSET.2017.0607329, PP 122-127

[15] B. Abinaya "An Intrusion Detection System MANET", DOI:10.15680/IJIRSET.2017.0602098, PP 1-6

[16] T.S. Urmila and R. Balasubramanian "A Novel Framework for Intrusion Detection Using Distributed Collaboration Detection Scheme in Packet Header Data" International Journal of Computer Networks & Communications (IJCNC) Vol.9, No.4, July 2017 PP 15051-15057

[17] Dr.V.Suganthi, P. K. Manoj Kumar "Intrusion Detection System – A Literature Survey", A Journal of Nehru Arts and Science College, Research Article Vol 6 issue 1(2018), PP 1975-1982

[18] Philokypros P. Ioulianou, Vassilios G. Vassilakis, and Ioannis D. Moscholios, Michael D. Logothetis, "A Signature-based Intrusion Detection System for the Internet of Things" Conference: Information and Communication Technology Forum (ICTF) 2018, At Graz, Austria, 11-13 July 2018, PP 97-113

[19] K. Narayana Rao, Prof. K. Venkata Rao, Prof. Prasad Reddy, "A Comprehensive survey of Machine Learning for Intrusion Detection ", International Journal of Research in Advent Technology, Vol.7, No.2, February 2019 E-ISSN: 2321-9637, PP 22-25

[20] D. Selvamani and V. Selvi, "A Comparative Study on the Feature Selection Techniques for Intrusion Detection System", AJCST Vol. 8 No. 1 January-March 2019, PP 1-7