INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

INTRUSION DETECTION SYSTEM SURVEY

[1]VODNALA SREEJA, [2] Dr.B. SATHEESH KUMAR

[1] M. Tech Scholar,[2] Professor, Department of CSE,

JNTUH UNIVERSITY COLLEGE OF ENGINEERING, JAGTIAL, T.S., INDIA.

ABSTRACT

The Intrusion Detection System (IDS) is intended to be a software programme that serves as a security system and protective layer for the infrastructure. It also keeps an eye on the network and detects any suspicious activity. Internet usage is increasing at an exponential rate, which raises questions regarding how to safeguard digital information. The IDS technology has advanced significantly over time to keep up with the growth of computer crime. Hackers today employ a variety of techniques to access our computers' personal, secure data. Numerous intrusion detection approaches, tactics, and algorithms will serve as a defence against these threats. The primary objective of this essay is to provide a thorough analysis of the definition of intrusion detection, its history, life cycle, and intrusion detection techniques, as well as the various types of attacks, tools and techniques available, and difficulties associated with its implementations.

1. INTRODUCTION

All harmful network traffic and computer activity that a traditional firewall is unable to identify is detected by an intrusion detection system. This includes malware, host-based attacks including privilege escalation, unauthorised logins and access to sensitive files, network attacks against susceptible services, data-driven assaults against apps, and host-based attacks against hosts. Users require security to protect their systems from outside forces that are undesirable. One of the common security methods used to secure the network is the firewall technique. IDS are utilised by insurance companies, medical applications, credit card fraud, and network-related activities[1].

ISSN: 2057-5688

The following three components make up an IDS:

Sensors: - which detect system activity or network traffic and produce events.

Console: For controlling the sensors and keeping track of events and notifications,

The detection engine employs a set of rules to create alerts from the security events it has received and stores events logged by the sensors in a database.

Depending on the kind of sensor, where it is located, how the engine generates alerts, and other factors, an IDS can be categorised in a number of different ways. All three components are frequently bundled into a single appliance or device in straightforward IDS solutions[2].

2. LITREATURE SURVEY

Monitoring network assets to identify unusual behaviour and network abuse is the primary goal of intrusion detection. After the development of the internet, intrusion detection was initially implemented in the early 1980s. Since then, a number of things have happened to progress IDS technology to where it is now[3]. The study "Computer Security Threat Monitoring and Surveillance," written by James P. Anderson, a pioneer in information security and member of the Defense Science Board Task Force on Computer Security of the U.S. Air Force, is frequently credited with establishing automated IDS. With an increase in shared networks in the late 1980s, enterprise system administrators all around the world started using intrusion detection systems. IDS technology advanced in the 1990s in response to the rise in frequency and complexity of network attacks[4]. The development and current prominence of intrusion detection are both significantly influenced by big data. Given that the amount of data in the globe doubles every 20 months and that cloud-hosted databases are growing quickly, IDS is more crucial than ever. Threat Stack is proud to support the IDS community and play a significant part in its progress. The protection and monitoring of computer networks can be carried out using a number of techniques that offer a certain level of comfort with acceptable risks. Defence-in- Depth refers to

ISSN: 2057-5688

the extensive analyst training, strategically placed gear, and robust security policy that are required to accomplish this goal. We have resources at our disposal every day to accomplish this. Data is collected from routers, the host computer, firewalls, virus scanners, and an instrument called an intrusion detection system that is specifically made to detect known attacks (IDS)[5].

3. INTRUSION DETECTION

A form of security management solution for computers and networks is intrusion detection. An ID system collects and examines data from multiple computer or network systems to spot potential security lapses, such as intrusions (attacks from outside the organisation) and misuse (attacks from within the organization). ID makes use of vulnerability assessment, a technology created to evaluate the security of a computer system or network (also known as scanning)[6].

4. INTRUSION DETECTION SYSTEM

IDS is another name for burglar alarm. For instance, the lock system in the house guards against theft. However, if a lock is broken and someone tries to enter the house, the burglar alarm is what notices the breakage and warns the owner by sounding an alarm. Additionally, firewalls are quite effective in filtering the incoming Internet traffic to avoid the firewall[7]. For instance, external users can access the Intranet by phoning using a modem that is set up in the organization's private network; the firewall is unable to identify this type of access.

Intrusion detection systems can be broadly categorised as follows:

A. Host-based IDS

Installed on the host that has to be watched are a Host Intrusion Detection System (HIDS) and software programmes. The agents keep an eye on the operating system and record information in log files or set off alarms. Only the specific workstations with installed agents can be monitored. Critical servers are monitored for intrusion attempts using host-based IDS systems[8]. Host-based IDS monitors the local system

ISSN: 2057-5688

for signs of intrusion. Host-based systems place a high value on audit trails. The data gives the intrusion detection system the ability to identify subtle patterns of abuse that would be hidden at a higher level of abstraction. Host-based Intrusion Detection Systems' benefits

Verifies whether an attack was successful or unsuccessful.

Near real-time detection and response to assaults that a network-based IDS misses

Does not need additional hardware; less expensive entry level

Host-based Intrusion Detection Systems have the following drawbacks: Difficult to assess the intrusion attempts on numerous machines

Large networks with many operating systems and configurations can be exceedingly challenging to maintain.

Attackers may disable it once the system has been compromised.

B. Network Based IDS

Network Appliances (or Sensors) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface make up Network Intrusion Detection Systems (NIDS). The IDS is positioned along a network segment or boundary, where it keeps track of all traffic. Instead of obtaining data from each individual host, these systems gather data from the network as a whole. As packets move via the network, the NIDS checks for network assaults. Because the monitors are transparent, it is less likely that an enemy will be able to find them and disable their capabilities without making any effort[9,10]. On every host in the network under protection, Network Node IDS (NNIDS) agents are installed. Network-based IDS fall under one of two categories, depending on how they operate: Pattern matching IDS and statistical anomaly IDS Network-based intrusion detection systems have the following benefits: Lower Total Cost of Ownership

Detect network-based threats more easily

ISSN: 2057-5688

Keeping track of evidence Real-time detection and prompt action Recognizing failed attacks

Network-based intrusion detection systems have the following drawbacks: Inability to decrypt encrypted packets Need for access to all monitored traffic

C. Application Based IDS

A unique subset of Host-Based IDS (HIDS), Application-Based IDS examines the events taking place inside a software application. The application's transaction log file is the most typical information source for application-based IDS.

Benefits of AIDS:

Aware of particular users

Observable user-application interaction; Operable even when incoming data is encrypted

AIDS's negative effects:

Less able to detect software manipulation and more prone to attack

5. INTRUSION DETECTION ATTACKS

Attacks known as denial-of-service (DOS) Denial of service (DoS) attacks generally fall into two categories: flooding and flaw exploitation. Flooding assaults are frequently easy to execute. For instance, the ping command alone can be used to execute a DoS assault. As a result, the victim will receive an excessive amount of ping packets. If the attacker has access to more bandwidth than the victim does, the victim will be swiftly and easily overcome. Another illustration is a SYN flood attack, which floods a victim with TCP/SYN packets that have a faked source address. The victim will send a TCPSYN/ACK packet and wait for an ACK response, which will force the victim to open partially closed TCP connections. The victim will eventually

ISSN: 2057-5688

run out of resources waiting for ACKs from an absent host because the ACK never arrives[11].

B. Eavesdropping Attacks: This is the attacker's plan to obstruct communication. This assault can be carried out via email or phone lines.

C. Spoofing Attacks - This attacker assumes the identity of another user to alter data and profit from nefarious activities taking place on the network. One typical instance is IP spoofing, in which the system interacts with a reliable user and grants access to the attacker.

D. User to root assaults (U2R) or intrusion attacks - An intruder attempts to enter the system or navigate the network. A classic intrusion assault known as a buffer overflow occurs when a web service receives more data than it has been designed to manage, which results in data loss.

E. Logon Abuse Attacks - By ignoring the authentication and access control procedures, a logon abuse attack would give a user extra benefits.

F. Attacks at the Application Layer - The attacker focuses on the limitations of the Application Layer.

6.TOOLS IN INTRUSION DETECTION

A variety of organisational security objectives are addressed by an intrusion detection device now on the market. The topic of security tools is covered in this section.

SNORT

Open source software that is lightweight is called Snort. To characterise the traffic, Snort uses a versatile rule-based language. It stores the packet in human readable form after receiving an IP address. Snort can identify tens of thousands of worms, attempts to exploit vulnerabilities, port scans, and other suspicious activity through protocol analysis, content searching, and different pre-processors.

The Suricata

Suricata competes most directly with Snort among the IDS/IPS solutions currently on the market. This system's design is comparable to Snort's, it relies on signatures similar to Snort, and it can even use the same Emerging Threat rule set and VRT Snort rules as Snort. Suricata has some catching up to do in this area because it is more recent than Snort. This is the closest free programme available to run on a business network if Snort is not an option in your company.

The OSSEC-HIDS

Open source software that is free to use is called OSSEC. It utilises a Client/Server design and is compatible with most major operating systems. The server can receive OS logs from OSSEC for analysis and storage. It is employed by ISPs, colleges, strong log analysis engines, and data centres. HIDS monitors and analyses firewalls and authentication logs.

With OpenWIPS-NG

Free wireless IDS/IPS called OpenWIPS-NG is supported by a server, sensors, and interfaces. It is powered by common hardware. This solution, developed by the creator of Aircrack-NG, employs a lot of the features and services that are currently included in Aircrack-NG for scanning, detection, and intrusion prevention. An administrator can download plug-ins for extra functions because OpenWIPS-NG is modular. Although the documentation isn't as thorough as that of some other systems, it nevertheless enables businesses to do WIPS on a shoestring budget.

7. COMPARISION OF DIFFERENT TOOLS AND TECHNOLOGY

The study, which was funded by grants from the Natural Sciences and Engineering Research Council of Canada and Dalhousie University's Electronic Commerce Executive Committee, revealed that in four of the five categories for insider traffic, Dragon outperformed or tied with the three open source systems. It caught at least 50% or more of the attacks in each category, with the exception of one. Furthermore, many of these attacks were stopped with a two confidence level. Only one of the eight active attacks was blocked by the denial of service category. In the log entries, 73% of the attack-related data was level 2[13,14].

Although Snort struggled in the other 3 categories, it once again did well in the DOS and Probe areas, catching more than 50% of the attacks in each. Its attack-related information was at confidence level 2 for 99% of the time. This research has demonstrated that none of the systems were able to identify even certain outdated attacks. It also demonstrated that assaults based on the misuse of perfectly lawful features could not be the fault of intrusion detection systems. The design and construction of operating systems still has flaws. The effectiveness of these technologies under attacks that are intended to bring down intrusion detection systems itself will be the subject of future study[15]. The School of Future Studies & Planning demonstrated that there are numerous solutions available on the market now to aid businesses in defending against the inescapable network and system attack. Only two of numerous resources that can be used to improve visibility and control inside a business computing environment are IDS and IPS technologies. IDS and IPS are to offer a foundation of technology that satisfies the need for tracking, identifying network threats to detect through IDS systems' logs and stopping an activity through IPS systems. It's a terrific idea to employ IDS, IPS, or both in network environments if the host has crucial systems, sensitive data, and stringent compliance requirements[16].

The firewall and intrusion detection systems both need to be enhanced, according to the International Journal of Computer Science and Information Technologies, in order to provide reliable network security. They are challenging to administer and not dependable enough (particularly in terms of false positives and false negatives). It is strongly advised to use a combination of several types of intrusion detection systems to provide effective computer security[17]. However, these technologies must be developed in the upcoming years due to rising corporate security demands and technological advancements that enable more effective operation detection systems. In order to facilitate a fair comparison of firewall and intrusion detection systems and to help concentrate research in this area on emerging trends like intrusion prevention systems, this paper offered a new perspective on network research that included types of firewalls and types of intrusion detection that are necessary, complete, and mutually exclusive.

8. CONCLUSION

This paper's main goal is to give an overview of the value and need for intrusion detection systems. The whole research of IDS kinds, life cycles, different domains, forms of attacks, and tools is provided in this work. IDS are growing crucial for current day network user and business security. The term "IPS" refers to security prevention methods. The stages and developed phases of the lifecycle are shown. There are still more obstacles to conquer. Additional strategies can be employed in addition to those expressly illustrated for anomaly and misuse detection. IDS will be improved utilising selective feedback techniques and a comparative analysis of a few well-known data mining algorithms that have been applied to IDS in the future.

9. REFERENCE

1. Aldwairi, M, Abu-Dalo, AM & Jarrah, M 2017, 'Pattern matching of signature-based IDS using Myers algorithm under MapReduce framework', EURASIP Journal on Information Security, vol. 2017, no. 1, P. 9.

2. Aldwairi, M, Conte, T & Franzon, P 2005, 'Configurable string matching hardware for speeding up intrusion detection', ACM SIGARCH Computer Architecture News, vol. 33, no. 1, pp. 99-107.

3. Alicherry, M, Muthuprasanna, M & Kumar, V 2006, 'High speed pattern matching for network IDS/IPS', Proceedings of the 2006 IEEE International Conference on Network Protocols, pp. 187-196.

4. Al-ramahi, N, Hnaif, AA & Awad, K 2019, 'Advanced Weighted Exact Matching Algorithm (AWEMA)', Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), IEEE pp. 141-144.

5. Ananth, J, Balakrishnan, S & Premnath, S 2018, 'Logo based pattern matching algorithm for intrusion detection system in wireless sensor network', International Journal of Pure and Applied Mathematics, vol. 119, no. 12, pp. 753-762.

6. Arslan, AN, He, D, He, Y & Wu, X 2015, 'Pattern matching with wildcards and length constraints using maximum network flow', Journal of Discrete Algorithms, vol. 35, pp. 9-16.

7. Baker, ZK & Prasanna, VK 2005, 'High-throughput linked-pattern matching for intrusion detection systems', Proceedings of the 2005 ACM symposium on Architecture for networking and communications systems, pp. 193-202.

8. Barajas-García C, Solorza-Calderón, S & Álvarez-Borrego, J 2016, 'Classification of fragments of objects by the fourier masks pattern recognition system', Optics Communications, vol. 367, pp. 335-345.

9. Bolotnikova, A, Demirel, H & Anbarjafari, G 2017, 'Real-time ensemble based face recognition system for NAO humanoids using local binary pattern', Analog Integrated Circuits and Signal Processing, vol. 92, no. 3, pp. 467-475.

10. Bouzelata, Y, Kurt, E, Chenni, R & Altın, N 2015, 'Design and simulation of a unified power quality conditioner fed by solar energy', International journal of hydrogen energy, vol. 40, no. 44, pp. 15267-15277.

11. Brodie, BC, Taylor, DE & Cytron, RK 2006, 'A scalable architecture for high-throughput regular-expression pattern matching', 33rd International Symposium on Computer Architecture (ISCA'06), pp. 191-202.

12. Busch, C 2019, 'Standards for biometric presentation attack detection', in Handbook of Biometric Anti-Spoofing, Springer, pp. 503-514.

13. Chhabra, S & Durham, DM 2019, Cross-domain Security in Cryptographically Partitioned Cloud, Ed: Google Patents.

14. Cirani, S, Ferrari, G & Veltri, L 2013, 'Enforcing security mechanisms in the IP-based internet of things: An algorithmic overview', Algorithms, vol. 6, no. 2, pp. 197-226.

15. Dey, H, Islam, R & Arif, H 2019, 'An Integrated model to make cloud authentication and multi-tenancy more secure', International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), pp. 502-506.

16. Dharmapurikar, S & Lockwood, J 2005, 'Fast and scalable pattern matching for content filtering', Symposium on Architectures for Networking and Communications Systems (ANCS), pp. 183-192.

17. Gubbi, J, Buyya, R, Marusic, S & Palaniswami, M 2013, 'Internet of Things (IoT): A vision, architectural elements, and future directions', Future generation computer systems, vol. 29, no. 7, pp. 1645-1660.

18. Hamsaveni, R, Gunasekaran, G & ME, P 2016, 'A secured pattern matching technique for intrusion detection system in wireless sensor network', Algorithms, vol. 6, no. 3.

19. Hudaib, A, Suleiman, D & Awajan, A 2016, 'A fast pattern matching algorithm using changing consecutive characters', Journal of Software Engineering and Applications, vol. 9, no. 08, P. 399.

20. Janani, R & Vijayarani, S 2016, 'An efficient text pattern matching algorithm for retrieving information from desktop', Indian Journal of Science and Technology, vol. 9, no. 43, pp. 1-11.

21. Jiang, L, Li, Y & Chen, G 2018, 'Research on a pattern-matching algorithm for the network security system', 11th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), pp. 1-9.

22. Joseph, L & Mukesh, R 2019, 'Securing and self recovery of virtual machines in cloud with an autonomic approach using snapshots', Mobile Networks and Applications, pp. 1-9.

23. Kasinathan, P, Pastrone, C, Spirito, MA & Vinkovits, M 2013, 'Denial-ofService detection in 6LoWPAN based internet of things', IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob), pp. 600-607.

24. Kaviya, K, Shanthini, K & Sujithra, M 2019, 'Evolving cryptographic approach for enhancing security of resource constrained mobile deviceoutsourced data in cloud computing', vol. 5, pp. 2456-3307.