International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 2, January-February 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

An Assessment of Intrusion Detection System (IDS) and Data-Set Overview: A Comprehensive Review of Recent Works

Mohammed I. Alghamdi

Department of Computer Science, Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia

ABSTRACT

Millions of people worldwide have Internet access today. Intrusion detection technology is a modern wave of information technology monitoring devices to deter malicious activities. Malware development (malicious software) is a vital problem when it comes to designing intrusion detection systems (IDS).

The key challenge is to recognize unknown and hidden malware, because malware writers use various evasion techniques to mask information to avoid IDS detection. Malicious attacks have become more sophisticated and Furthermore, threats to security have increased, including a zero-day attack on internet users. Through the use of IT in our daily lives, computer security has become critical. Cyber threats are becoming more complex and pose growing challenges when it comes to successful intrusion detection.

Failure to prevent invading information, such as data privacy, integrity and availability can undermine the credibility of security services. Specific intrusion detection approaches were proposed in the literature to combat computer security threats.

This paper consists of a literature survey of the IDS that uses program algorithms to use specific data collection and forensic techniques in real time. Data mining techniques for cyber research are introduced in support of intrusion detection.

KEYWORDS: *Cybersecurity, Network security, Signature-based, identification, Information technology (IT)*

How to cite this paper: Mohammed I. Alghamdi "An Assessment of Intrusion Detection System (IDS) and Data-Set Overview: A Comprehensive Review of Recent Works" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-2, February 2021, pp.979-982, URL: www.ijtsrd.com/papers/ijtsrd35730.pdf

IJTSRD35730

1. INTRODUCTION

In the past, cyber criminals were primarily focused on banks' clients, bank accounts manipulation or theft of credit cards. But the new generation is reckless, threatening banks themselves and sometimes trying to take millions of dollars in one attack [1].

The new generation of malware Which is why zero-day attacks have become the top priority. Cybercrimes have demonstrated the ease with which it is possible to transmit cyber threats worldwide, as a simple hack may destroy a company's critical services or facilities.

Intrusion is also known as malicious internet practices. An intrusion is characterized as an operation contrary to the security policy of the network [2]. Due to the growing complexity and larger size of operating systems and applications, there are various sources of threat, including software bugs. Intruders not allowed to access these data who deprive network users of valuable and private data.

Firewalls are software or hardware systems installed between two or more computer networks to avoid attacks performed through the use of rules and policies that have been developed in such networks isolation.

Firewalls are quite clearly not sufficient to secure a network entirely, because attacks from outside the network are avoided, whereas attacks inside the network aren't adequate. It is where intrusion detection systems are operated by the IDSs. IDSs are used to deter attacks, recover losses or assess security problems in order to avoid their reproduction [3].

The IDS is software and hardware that is used to detect unauthorized use or target an application or a network of telecommunications to resolve the differences between firewall and anti-virus systems.

An IDS provides user behavior monitoring and analysis, system configuration and vulnerabilities can be inspected, critical system and data security files can be evaluated, trends in activity can be statistically analyzed in line with known attacks, behavior analysis and system auditing [4].One benefit of the IDS is its ability to record an organization's intrusion or danger, providing the basis for informing the public through device logs about the current patterns of attack.

Intrusion detection systems are also considered to be a fundamental component of production system security that includes mission-critical information, IP information and other digital properties. Without an IDS, a business's production systems and data are vulnerable to cyber attacks and other crime. When unauthorized individuals break down the records, the entire structure of the company collapses easily, thus leaving the company with great uncertainty about its viability [5].

An IDS has traditionally supported administrateurs in detecting intrusions to deter threats, including VPNs,

malware security, firewalls or controlled IT, as part of a robust safety strategy. But the position of IDS is rising slowly. Hackers ' innovations for hiking a network and administrators ' countertechnology in order to deal with these attacks have outperformed the scope and ability of IDS. It has been all but old-fashioned for an IDS to track threats in real time and zero day[6].

Intrusion detection systems (IDS) are among the latest security tools. Based on their characteristics, I can classify them into different types, such as their detection and prevention strategies, their architecture, or the detection range[7]. In fact, given their effectiveness, most IDS have two problems: the large number of false positives and negatives. The false positives, the false alarms, are produced when the IDS detects normal activities as intrusions, while the false negatives correspond to non-detected attacks or intrusions, and no warning is generated[8].

Three types of IDS-detected computer attacks exist:
(i) attacks by a scan device, (ii) attacks by a denial of service and (iii) intrusion attacks[3]. Each of the three types of computer attacks has distinct signatures and behavior-IDS is scheduled for alarm evaluation, detection and detection.

2. Literature Review

In the literature, there are several techniques available to detect the intrusion behavior. It is also very important to maintain a high degree of protection and ensure that communication between different organizations is secure and trustworthy. Nonetheless, safe Internet and other networks are still at risk of attack and misuse. Therefore, intrusion detection systems have become a computer and network protection feature that is essential. Different methods in intrusion detections are used, but none of the systems is still fully unreliable so far [9]. Intrusion detection has been receiving a lot of attention among researchers in recent times as it is commonly used to maintain protection within a network. Here I present some of the intrusion detection methods used.The fundamental task of the detection system for intrusion is to identify network behaviors as normal or abnormal while reducing misclassification [10-12].

As stated by Owens and Levary, intruders' detection systems have generally been established with the aid of expert system technology. But in building systems, which are difficult to deal with, lacking clear user interfaces and unpleasant to use in real-world conditions, experts from the Intrusion Detection Network (IDS) have been biased [13].

Numerous research papers on IDSs for technologies such as mobile ad hoc networks (MANETs) [14-16], wireless sensor networks (WSNs) [17-19], and cloud computing [20] and cyber-physical systems (CPS) [21] have been published over the past few years. Zarpelao et al. [22] provide an IDS analysis.

They discuss IDS placement strategies and detection methods in their survey article. I also pose common security threats and how to identify those using IDSs. In addition, they present a review of the common validation strategies used in intrusion detection methods and discuss open research issues and trends in the future.

In signature-based approaches, IDS detect attacks when the device / network activity matches an IDS attack symbol. If any device or network behavior is consistent with the stored patterns / signatures, an alert is activated. This approach is very effective and efficient in the identification of known threats and is easily understood by its process. Nonetheless, in detecting new attacks and variants of known attacks this strategy is failing, as a corresponding signature for such attacks is still unknown[23-24].

The following advantages are provided by signature detection methods: low false alarm rate, simple algorithms, and easy database creation for attack signatures, quick implementation and usually minimum computer resource use.

Several drawbacks:

- Problems in adding different forms of attack details (when adding the attack signature database, as appropriate).
- New threats that are unknown cannot automatically be identified. The Attack Signature database must be continuously updated.
- Maintaining IDS is necessarily linked to the detection and patching of safety holes that are time consuming. [23-24].

IDSs based on anomalies compare system behaviors at a time with a normal behavioral profile and alarm when an abnormality crosses a threshold. Nonetheless, something that does not match a normal behavior is considered an violation, and it is not a easy task to grasp the whole spectrum of normal conduct. Generally the false positive rates of this process are high [22, 25]. Researchers usually construct the standard behavior profile with statistical techniques or machine learning algorithms.

Arman Tajbakhsh suggested an IDS-based system for data mining techniques. In the Association Based Classification (ABC) system, the classification engine is, in turn, the core part of the IDS [26].

The classification proposed using fuzzy association rules to create classifiers. Such tests were used to assess the validity of every new sample (which must be categorized) and to establish the sample mark as the best corresponding class rule collection. A procedure that reduces items that can be included in the rules extracted is also proposed to reduce the time the rule induction algorithm takes. The layout has been checked with the KDD-99 dataset. The findings indicate that the overall detection rate of known attacks was high and the false positive rate was low, even though the results of the unknown attacks were not obvious. [26].

3. Methodology

I reviewed 20 works published in the last 16 years between 2002 and 2018 proposing IDS solutions in this study. I used a taxonomy focused on features such as the placement technique, the method of detection and the threat of security.

4. Results and Discussion

Most published documents claiming to evaluate IDSs are performed as comparisons rather than assessments. Assessment should be viewed as assessing the extent at which a given IDS achieves defined performance targets. There are many problems in IDS and need to be solved, such as poor detection capacity against unknown network attack, high false alarm rate, and inadequate analytical capability [10-12].

IDS systems distinguish between requirements. In the first place, IDSs can be distinguished on the basis of the type of operations, traffic, transactions or structures they control.

IDSs can be divided into network, host and application-based groups of IDS. Network-based IDS are known as network-based IDSs that monitor Network backbones and check for intrusion signatures, while those on hosts identify, track and host host-based IDSs.

Many IDSs only monitor applications directly and are classified as application-based IDSs. (Such care is usually restricted to broad applications like database systems, content management systems, accounts, etc.)[27].

Different approaches of IDS control:

4.1. Network-based IDS Characteristics:

Network IDSs are capable of controlling and overloading a large network with only few well-placed nodes or computers. Network-based IDSs are mainly passive tools to control the ongoing activity of the network without excessive interference. It is easy to defend against attack and can also not be detected by attackers; it also takes little effort to mount and use existing networks. Network-based IDS does not monitor and analyze all traffic on large, busy networks and therefore neglect attacks during peak traffic.

In addition, network-based IDSs cannot track switch-based (high-speed) networks effectively. Network based IDSs are usually unable to analyze encrypted data or disclose attack success or failure. Therefore, network IDSs require the involvement of manual network managers to assess the impact of reported attacks to a certain extent [28-29].

4.2. Host-based IDS Characteristics:

IDS can analyze the host activities in a high degree of detail; it can periodically analyze the processes and/or users engaged in malicious activities. Whereas they are each capable of focusing on a single host, most domain-based IDS systems have an agent console model where agents work on (and monitor) individual hosting systems and report to a single centralized server (so that a multi-host console can set up, track and aggregate data). Host-based IDSs can detect undetectable attacks on network-based IDS and accurately calculate the outcome of attacks. Host-based IDSs use host-based encryption services to explore encrypted transport, data, storage and operation.

Data collection is per host; writing to logs or recording activities requires network traffic and can reduce network performance. Clever server-based attackers can also target and disable host-based IDSs. DoS attacks can thwart server based IDSs (because they can prevent traffic from reaching host where it is running or because they may prevent reporting on such attacks to a console otherwise in a network). In particular, a host-based IDS uses the server that runs these Systems for process time, energy, memory and other resources

5. Conclusion

Cyber threats are becoming more complex and pose growing challenges when it comes to successful intrusion detection. Failure to prevent invading information, such as data privacy, integrity and availability can undermine the credibility of security services.

In order to protect data during transmission, network security measures were required. Safety of the network includes securing a network from unauthorized access and risks. Network administrators / Information Security experts have a duty to take proactive measures to protect their networks from potential threats to security. Organizations incorporate Intrusion Detection Systems (IDS) to detect unauthorized behaviors in the network or on individual machines. Detection of intrusion has been studied for nearly 20 years. Intrusion Detection Systems track malicious/unauthorized network activities, record information on such activities / send alerts, take steps to stop them / drop packets.

References

[1] Ablon L, Libicki MC, Golay AA. Markets for cybercrime tools and stolen data: Hackers' bazaar. Rand Corporation; 2014.

[2] Awan JH, Memon S, Khan RA, Noonari AQ, Hussain Z, Usman M. Security strategies to overcome cyber measures, factors and barriers. Eng. Sci. Technol. Int. Res. J. 2017; 1(1):51-8.

[3] Anderson JP. Computer security threat monitoring and surveillance. Technical Report, James P. Anderson Company. 1980.

[4] Chen Q, Abdelwahed S, Erradi A. A model-based validated autonomic approach to self-protect computing systems. IEEE Internet of things Journal. 2014; 1(5):446-60.

[5] Ashoor AS, Gore S. Importance of intrusion detection system (IDS). International Journal of Scientific and ngineering Research. 2011; 2(1):1-4.

[6] Jabez J, Muthukumar B. Intrusion detection system (IDS): anomaly detection using outlier detection approach. Procedia Computer Science. 2015; 48:338-46.

[7] Debar, H., and Jouni V. "Intrusion detection: Introduction to intrusion detection and security information management." Foundations of security analysis and design III. Springer, Berlin, Heidelberg, 2005. 207-236.

[8] Debar, H., Marc D., and Andreas W. "IN Revised Taxonomy Heart Intrusion Detection Systems." Annals of the Telecommunications, Flight 55: 7-8.

[9] Kadam PU, Deshmukh M. Various approaches for intrusion detection system: an overview. International Journal of Innovative Research in Computer and Communication Engineering. 2014 Nov; 2(11).

[10] Wilkison M. IDFAQ: how to evaluate network intrusion detection systems. Retrieved from SANS Technology Institute: https://www.sans.org/security-resources/idfaq/how-toevaluate-network-intrusion-detection-systems/8/10. 2002.

[11] Mohammadpour L, Hussain M, Aryanfar A, Raee VM, Sattar F. Evaluating performance of intrusion detection system using support vector machines. International Journal of Security and Its Applications. 2015 Sep; 9(9):225-34.

[12] Kuang F, Xu W, Zhang S. A novel hybrid KPCA and SVM with GA model for intrusion detection. Applied Soft Computing. 2014 May 1; 18:178-84.

[13] Peiravi A. Application of string matching in Internet Security and Reliability. Marsland Press Journal of American Science. 2010; 6(1):25-33.

[14] Mishra A, Nadkarni K, Patcha A. Intrusion detection in wireless ad hoc networks. IEEE wireless communications. 2004; 11(1):48-60.

[15] Anantvalee T, Wu J. A survey on intrusion detection in mobile ad hoc networks. InWireless Network Security. Springer, Boston, MA. 2007 (pp. 159-180).

[16] Kumar S, Dutta K. Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges. Security and Communication Networks. 2016 Sep 25; 9(14):2484-556.

[17] Farooqi AH, Khan FA. Intrusion detection systems for wireless sensor networks: A survey. In International Conference on Future Generation Communication and Networking. Springer, Berlin, Heidelberg. 2009; pp. 234-241.

[18] Abduvaliyev A, Pathan AS, Zhou J, Roman R, Wong WC. On the vital areas of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys & Tutorials. 2013; 15(3):1223-37.

[19] Butun I, Morgera SD, Sankar R. A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials. 2013; 16(1):266-82.

[20] Modi C, Patel D, Borisaniya B, Patel H, Patel A, Rajarajan M. A survey of intrusion detection techniques in cloud. Journal of network and computer applications. 2013; 36(1):42-57.

[21] Mitchell R, Chen IR. A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys (CSUR). 2014 Apr 1; 46(4):55.

[22] Zarpelão BB, Miani RS, Kawakani CT, de Alvarenga SC. A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications. 2017; 84:25-37.

[23] Vacca, J. Computer and Information Security Handbook. Morgan Kaufmann, Amsterdam, 2013.

[24] Liao HJ, Lin CH, Lin YC, Tung KY. Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications. 2013; 36(1):16-24.

[25] Scarfone, K. and Mell, P. "Guide to intrusion detection and prevention systems (IDPS)", Technical report, National Institute of Standards and Technology, Special Publication, 2007; 80-94.

[26] Tajbakhsh A, Rahmati M, Mirzaei A. Intrusion detection using fuzzy association rules. Applied Soft Computing. 2009; 9(2):462-9.

[27] Jyothsna VV, Prasad VR, Prasad KM. A review of anomaly based intrusion detection systems. International Journal of Computer Applications. 2011 Aug; 28(7):26-35.

[28] Kreibich C, Handley M, Paxson V. Network intrusion detection: Evasion, traffic normalization, and end-to-end protocol semantics. InProc. USENIX Security Symposium 2001 (Vol. 2001).

[29] Ashour A. importance of Intrusion Detection System (IDS). International Journal of Scientific Engineering Research, 2005; 1-7.