THE ROLE OF INTRUSION DETECTION/PREVENTION SYSTEMS IN MODERN COMPUTER NETWORKS: A REVIEW

Suman Thapa
Department of Information Systems
St. Cloud State University
St. Cloud, MN 56301, USA
Sthapa2@go.stcloudstate.edu

Akalanka Mailewa Dissanayaka
Department of Computer Science and IT
St. Cloud State University
St. Cloud, MN 56301, USA
amailewa@stcloudstate.edu

Abstract

The emergence of new devices that make use of the Internet as their primary utility has made network security one of the most important domains in the world today. Intrusions in computing environment are very prevalent and causing a lot of problems for people, business or government that deem to keep their information private. As a result, data security has become a prominent issue that needs to be addressed in an urgent manner. An intrusion, in terms of computing, can be defined as the act of compromising a computer system by breaking the security of such system. Everyday millions of computers are being victims of such practice causing businesses to lose money by exposing their private and confidential information to their corporate competitions. As a result, network security has become very important for computer users and organizations. To prevent unauthorized access to systems, a wide number of intrusion detection and prevention tools have been created that allow to track, monitor, comprehend and detect unwanted traffic on a network or a networking device. Introduced in the early 2000s, IPS (Intrusions Prevention Systems) and IDS (Intrusions Detection System) are the main widely used intrusion detection and prevention tools. Different types of security tools such as firewalls, antivirus software, antispyware, antimalware, etc. are readily available to protect the system but they fail to provide security to the system against the threats because of their limited functionalities and capabilities. To overcome such limitations, the Intrusion Detection and Prevention System (IDPS) comes into play. This paper describes the main functions of IDS and IPS in network security. It also provides an insight into the IPS and IDS tools that could be implemented to improve the security of the information systems. This paper also discusses what the IDS and IPS are, their working mechanisms and their roles in providing the strongest protection against the threats to ensure the security of the system.

Keywords: IDS, IPS, Threats, Malware, Information Security, Intrusion Detection, Intrusion Prevention, Firewalls, Computer Networks, Vulnerabilities.

1. INTRODUCTION

Intrusions in computing jargon can be defined as the act of compromising a computer system by breaking the security of such system. Everyday millions of computers are victims of such practice causing businesses to lose money by exposing their private information to corporate competitions. As a result, network security has become very important for computer users and organizations [1][2]. To prevent unauthorized access to systems, a wide number of intrusion tools have been created that allows to track, monitor, apprehend and detect unwanted traffic on a network or a device. On these numerous intrusions tools, introduced in the early 2000s, the main widely used are IPS (Intrusions Prevention Systems) and IDS (Intrusions Detection System). Both of them inspect network packets and block suspicious ones, as well as alert administrators about attack attempts [3]. An IPS can be defined as an active in-network control system that prevent incoming threats and stop attacks in progress whereas an IDS is a detection and monitoring tool that alerts users of potential malicious traffic [4]. In this paper, IDPS is referred to as the combination of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

1.1 HISTORY AND DEVELOPMENT

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) were first introduced in 1986 as an academic paper written by Dorothy E. Denning; the paper was titled “An Intrusion-Detection Model” [5]. By doing so, the Stanford Research Institute (SRI) took that opportunity and developed the Intrusion Detection Expert System (IDES). The IDES system used statistical anomaly detection, signature profiles of users and host systems to detect nefarious network behaviors.

From 2000 to 2005; intrusion detection was preferred over intrusion prevention. This was because, in the early 2000s, new threats like SQL injection and cross site scripting attack (XSS) were becoming popular and these attacks passed right by the firewall [6]. Firewall was very effective for preventing against threat in the 1990s but, with new threats, IDS become the most secure practice [7]. At that time, the market for IPS was very low because most organizations were worried that IPS could probably stop harmless anomalous traffic from prospects. IPS works by sitting in-line between an organization’s network and the internet compared to the IDS that works by sitting to the side and mirroring all the traffic that comes into the network. The main reason behind preferring IDS over IPS was because IDS would warn or alert the organization when it finds malicious activity, then they would take the right measures to get rid of the threat [8].

The adoption of IPS didn’t start growing until the latter part of 2005 when more merchants started supporting it. In that time, signatures were written to detect exploits and no vulnerabilities. The idea was that for every vulnerability, there could be a hundred ways to exploit it [5][9]. When criminals detected a vulnerability, they could generate more than a

hundred different ways to exploit it, causing IDS merchants to write a hundred or more different exploit signatures. So, since IPS is in line, consumers were concerned that all those signatures would slow down the network as each connection would have to be checked. Because of that concern, IPS merchants started to create only one signature that would work with each vulnerability regardless of how many exploits were connected to it. Merchants found that an IPS or an IDS that have more than 3500 signatures is apt to hinder its performance [5][10]. To this day, both IDS and IPS keep changing and developing as attackers change the techniques used to break into networks.

1.2 Intrusion detection system

The term intrusion refers to interrupting someone without permission. In the context of computing, intrusion refers to an attempt of accessing computer system resources without any permission with an intention of causing incidental damage [11]. Basically, Intrusion Detection refers to any kind of mechanism to detect such intrusive behavior and Intrusion Detection System (IDS) refers to a system that performs the process of intrusion detection automatically [12]. The IDS is responsible for monitoring the data traffic in the network and any suspicious activities against the network security. The system or network administrator of the network are alerted or reported if any threats or malicious activities are detected in the network [13]. Hence, the main purpose of the IDS is to detect and report the intrusion attempts to the concerned parties. The IDS employ different types of tools and techniques to detect suspicious activities both at the host and the network level. The IDS can be divided into two main types such as Host-Based Intrusion Detection Systems (HIDS) and Network-Based Intrusion Detection Systems (NIDS) [14].

1.3 Intrusion prevention system

Basically, it is a system that detects both intrusions and take responsive actions to mitigate such intrusions [15]. The IPS can be considered as a combination of IDS, firewalls, antiviruses, vulnerability assessment tools, etc. where IDS detect the intrusions in the network as well as the host level and the preventive measure tools (often implemented in hardware) prevent the network from various attacks [16]. Hence, the IPS not only detects an attack but it also responds to such attack automatically by adopting countermeasures such as logging off the user from the system, killing the process, shutting down the system, dropping the connection, etc [17]. Similar to IDS, the IPS can be divided into two main types such as Host-Based Intrusion Prevention Systems (HIPS) and Network-Based Intrusion Prevention Systems (NIPS).

Rest of the paper organized such that, first, it presents the background to give an idea of evolutionary development of IDS and IPS. Second, the methodology of inclusion and exclusion of reviewed literature. Third, the behavior of IDS and IPS in computer networks. Finally, the roles of IDS/IPS in computer networks with some example tools.

2. BACKGROUND

As this paper presents in the introduction section, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are not a new concept. They have evolved over time with the advancement of internet and complexity in computer security. There are many scholars who have worked on this topic dating back to the 1980s.

James P. Anderson's report [18] titled "Computer Security threat and monitoring and surveillance" was the base for all the reports regarding this field. In this paper, he introduced the idea of Intrusion Detection System. He has mentioned this system as a security audit trails. He further discussed a system that consists of tools that would come handy for computer system security personnel. This paper carefully explains the concept of Threat, Risk, Vulnerability and Attack. The design proposed the idea of monitoring users, user session builder and surveillance program. Since the paper is four decades old, the threat mostly considered is from users within the system. Hence, the paper can be considered the base of IDS reports and technically outdated. This paper does not discuss Intrusion Prevention System.

Nilotpal Chakraborty's paper [19] titled "Intrusion Detection System and Intrusion Prevention System: A comparative Study" compares the differences between IDS and IPS. In this paper, the author explains that the function of an IPS is to sit between networks and control traffic between the connection. The author explains that IPS denies all requests that the system deems a threat or malicious. The author explains that IDS works as a visibility tool. It sits on the side of the network and analyses the system security health. IDS is limited to error detection whereas IPS implements measures to make the system secure.

Lora O'Haver's blog [20] titled "IPS and IDS: Role and Function" gives a clear distinction between IPS and IDS functions. In her article, she writes that an IPS system should be able to stop potential attacks without affecting network performance. She mentions that IDS is an older approach to computer security, however there are some IDS systems that can be configured to respond to a threat just like an IPS system. She gives a brief explanation about identification techniques such as signature-based identification, Statistical anomaly-based techniques and rule-based techniques. In addition, she has provided factors that can make a system effective and efficient for IPS and IDS deployment which are Fail-safe Operation, Zero Downtime Maintenance, Accelerated Deployment, Out-of-band or Tap mode and visibility.

3. METHODOLOGY

3.1. Source of Information

The source of information are published articles, papers, journals and reports. The documents were thoroughly read, examined and scrutinized. Most papers explained the roles of IDS and IPS effectively and explained the differences between IDS and IPS.

3.2. Relevance of Information

Since numerous sources contributed to this paper, not all information were deemed fit for this paper. Some of the papers were outdated or old. As information technology, security and computer science evolves very quickly, not all information were deemed relevant. The roles discussed in these papers were analyzed thoroughly with present technology and only relevant roles were selected.

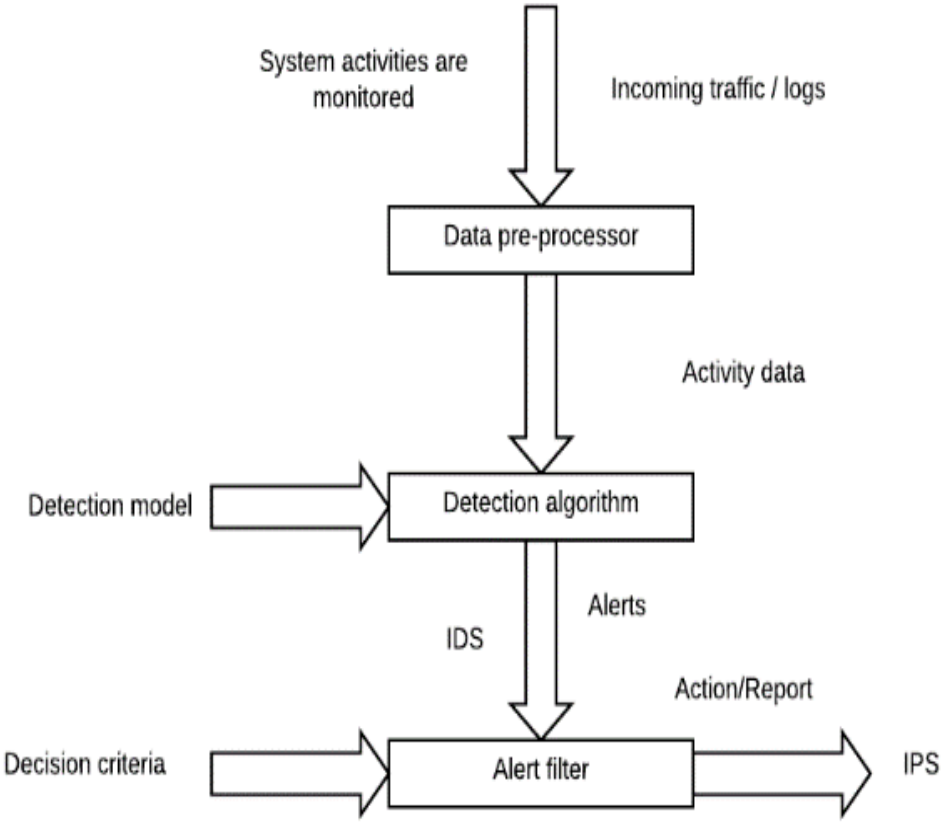

Fig. 1. Common Components of an IDS/IPS [23]

4. IDS AND IPS IN COMPUTER NETWORKS

In the network, the firewall plays a vital role by providing security to the network by allowing incoming and outgoing network traffic only on specified ports. The firewall is not built to detect the network traffic sent on a specified port or legitimate port or any sort of intrusion attempts or attacks [21]. For instance, a firewall rule allowing inbound access on TCP port 80 will allow remote access to an internal web server. An attacker could use the HTTP port to attack the web server. In this scenario, the IDS can determine the difference between the legitimate traffic (allowed connections) and attempted attack to the web server by making comparison between the signature of the web traffic and a database of well-known attack signatures. Here, the IDS plays a vital role by notifying the network administrator about such attack and alert him/her to take appropriate action accordingly [22]. On the other hand, the IPS plays a vital role by taking action on the attack attempt by taking an appropriate action automatically. For instance, dropping / closing the connection to the web server. Therefore, the IDS acts passively by generating logs and alerting the network administrator after the attack attempts or occurrence of malicious activities whereas the IPS actively monitors such activities and takes action against such activities to protect the network. Therefore, the IDS and IPS act as network level defenses to secure the computer network [23]. The main architectural overview of both the IDS and IPS in network intrusion detection and prevention is represented in the figure 1.

4.1. Basic Assumptions

Regarding the operations of IDS/IPS, it has to make following three basic assumptions [24]:

- System activities can be observed
- Normal and intrusive activities have distinct evidence
- The goal of an IDS/IPS is to detect the difference

4.2. Components of an IDS/IPS

The IDS/IPS system is composed of the following components [25].

1. **Data pre-processor:** The data pre-processor is responsible for collecting and formatting the data to be analyzed by the intrusion detection algorithm.
2. **Detection algorithm:** The detection algorithm detects the difference between “normal” or “legitimate” and intrusive network traffic on the basis of the detection model.
3. **Alert filter:** The alert filter estimates the severity of the intrusion based on the decision criteria and the detected malicious activities. The alert filter then alerts the network or system administrator and takes the responsive actions (usually blocking).

The IDS is composed of intrusion detection algorithm and alert filter in which rule sets are predefined in order to detect the threats or intrusions and generate the activity data / logs or alerts [26]. The IPS is deployed in-line in the network between the network components so that it can take appropriate actions against the malicious activities in the network [27]. It performs the same sort of monitoring and analysis activities as IDS does, but it not only detects the threats or intrusions but takes appropriate action on the intrusions such as closing the connection

5. FUNCTIONS OF IDS/IPS

As we already discussed the Intrusion Detection System (IDS) and the Intrusion Prevention System (IPS) are both network level security measures utilized in computer network globally. The major difference between IDS and IPS systems are how network environment are protected in terms of detection and prevention. Alerts are generated in IDS after the occurrence of a malicious attack and then reported to the network administrator [28][29]. Also, network administrators have the capability to disable the prevention features in IPS, making them to operate as IDS. In general, the role/function of IPS & IDS in Network security are assimilated. The IDS consist of four key functions namely, data collection, feature selection, analysis and action [30].

5.1 Data Collection

From this module, IDS receive data as input, save in the file and analyze them. Network based IDS collects and alters the data packets and in host-based IDS collects details like usage of the disk and processes of the system [31][32].

5.2 Feature Selection

To select a particular feature, large data is available in the network and they are usually evaluated for intrusion. For example, the Internet Protocol (IP) address of the source and target system, protocol type, header length and size could be taken as a key for intrusion [33].

5.3 Analysis

The data is analyzed to find the correctness. Rule based IDS analyze the data where the incoming traffic is checked against predefined signature or pattern. Another method is anomaly-based IDS where the system behavior is studied, and mathematical models are employed to it [34].

5.4 Action

It defines about the attack and reaction of the system. It can either inform the system administrator with all the required data through email/alarm icons or it can play an active part in the system by dropping packets so that it does not enter the system or close the ports [35].

Aside from monitoring and analyzing activities to identify suspicious activity, all IDS system perform the following general functions [36]:

- Document Information pertaining to the observed activity. The information can either be recorded locally or sent to the centralized log management server (SIEM).
- Provides notification about observed activity to security administrator. This notification referred to as alert can be in form of email, messages, pages, script etc. The notification message includes little details about the observed events. Additional information regarding the event, administrator is required to access the IDS.
- Generating of reports. All monitored activities or events are summarized in the report.

The distinct capabilities of IPS that differs from IDS is the ability to not only detect but also prevent or stop detected threat from being successful. Instead of just recording a suspicious activity, alert or inform an administrator, or report the violation to a central repository like the IDS, IPS is designed to be deployed inline on the network, close to the perimeter, and complement the work of the network firewall. While the firewall works to positively identify traffic that is allowed to move on towards the internal network, the IPS looks for dangerous incoming packets or traffic that violate specific rules or network policies. Once suspicious traffic is identified, the IPS takes action by automatically blocking the traffic, logging the attack, and adding the source IP address to the block list for a period of time [37]. Followings are the response techniques used by IPS.

- Detects and takes preventive measures against attacks.
- Ability to stop attack: The IPS can stop attack by aborting the attacker's network connection, obstructing access to the target user account or IP address.
- Change the Security Environment: The IPS has the capabilities to change other security control configuration in order to interrupt an attack. For example, network firewall configuration to deny access to the target system and the application of the latest patches to a system identified to be vulnerable by the IPS.
- Change the attack content: Some IPS offers the ability to remove the malicious content of an attack and render it harmless. For example, an email containing a malicious file attachment will be removed by the IPS and the recipients receives the clean email.

6. IDS AND IPS TOOLS

6.1 Snort

Created by Martin Roesch in 1998, Snort is a free and open source packet sniffer and logger which can be also be used as a network intrusion detection system (NIDS). In 2009, Snort entered InfoWorld's Open Source Hall of Fame as one of the "greatest open source software of all time". Snort detects various types of attacks and probes such as SMB probes, vulnerability exploit attempts, stealth port scans, and other suspicious behavior by employing rules-based logging that performs content pattern matching [38].

6.2 OSSEC

OSSEC is an open source host-based intrusion detection system (HIDS). It does log analysis, integrity checking, rootkit detection, time-based alerting and active response. It can respond to specific events or set of events by employing various commands and active responses. Standalone installation of OSSEC can be made to monitor a single host or it can be deployed in a server and installation on the others will be as agents. The communication between the server and the agents is encrypted to make it secure. The system administrator can add more other active response tools in addition to some predefined active response tools that comes with OSSEC [39]. In addition to its IDS functionality, it is commonly used as a SEM/SIM solution.

6.3 OSSIM

OSSIM is an acronym for Open Source Security Information Management system. A powerful set of open source security tools such as Snort, Nessues, Ntop, Nmap, etc. is integrated by OSSIM. It provides a comprehensive compilation of tools which grants network administrators with a detailed view over each and every aspect of networks, hosts, physical access devices, and servers [40].

6.4 Suricata

Suricata is an open source-based intrusion detection system which was developed by the Open Information Security Foundation (OISF). It can be run on both IDS and IPS modes. Like Snort, it is based on the predefined set of rules to detect various attacks and probes. The rate of false negative and false positive threat recognition is determined by the precision of the predefined set of rules in Suricata. [41].

6.5 Zeek (Bro)

Zeek is an open-source, Unix-based network intrusion detection system [42]. It detects intrusions by first parsing network traffic to determine its application-level semantics and then executing event-oriented analyzers that compare the activity with patterns deemed malicious.

6.6 Fragroute/Fragrouter

Fragrouter is a network intrusion detection evasion toolkit. It evades Network Intrusion. It helps to implement network security attacks such as Insertion, Evasion, and Denial of Service (DOS) etc. [43]. It helps an attacker launch IP-based attacks while avoiding detection.

6.7 BASE

The BASE is a PHP-based analysis engine to search and process a database of security events generated by various IDSs, firewalls and network monitoring tools. BASE is used as a web-based graphical interface tool to analyze the alerts which are generated by Snort. It was derived from the ACID project (Analysis Console for Intrusion Databases). BASE is a utility that is specific to Snort. [44].

6.8 Sguil

Sguil is an IDPS tool completely written in Tcl/Tk (Tool Command Language / Tool Kit) and built by network security analysts for network security analysts. The graphical interface that Sguil is an analysis interface provides makes it valuable to the end user. Sguil displays network packet information from various types of open source tools in real time to the end user. [45].

7. CONCLUSION

Different types of security tools such as firewalls, antivirus software, antispyware, antimalware, etc. are readily available to protect the system but they fail to provide security to the system against the threats because of their limited functionalities. To overcome such limitations, the Intrusion Detection and Prevention Systems comes into play. The IDS and IPS provide the functionalities to detect the attacks and prevent such attacks by implementing various approaches such as secure mobile agent, virtual machine; multilayer and distributed approach, high throughput string matching, to provide stronger and greater security against multiple security threats and attacks. This paper discusses what the Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are, their working mechanism and their roles in providing the strongest protection against the threats to ensure the security of the system. The IDS and IPS are two of the network security technologies available in the market to help fight the inevitable network and system attacks by detecting, tracking and identifying the network attacks through the logs of IDS systems, and preventing the negative consequences of such network attacks by implementing appropriate automatic action through the IPS systems. Hence, it is highly recommended to use IDS, IPS or both in a network environment to protect the system from theft and loss of confidential data as well as maintain the strict compliance regulations for the critical systems.

References

[1] Akintaro, Mojolaoluwa, Teddy Pare, and Akalanka Mailewa Dissanayaka. "DARKNET AND BLACK MARKET ACTIVITIES AGAINST THE CYBERSECURITY: A SURVEY." In The Midwest Instruction and Computing Symposium. (MICS), North Dakota State University, Fargo, ND, April 5-6 2019.

[2] Akalanka Mailewa Dissanayaka, Roshan Ramprasad Shetty, Samip Kothari, Susan Mengel, Lisa Gittner, and Ravi Vadapalli. 2017. A Review of MongoDB and Singularity Container Security in regards to HIPAA Regulations. In Companion Proceedings of the10th International Conference on Utility and Cloud Computing (UCC '17 Companion). ACM, New York, NY, USA, 91-97.

[3] Ashoor, Asmaa Shaker, and Sharad Gore. "Difference between intrusion detection system (IDS) and intrusion prevention system (IPS)." In International Conference on Network Security and Applications, pp. 497-501. Springer, Berlin, Heidelberg, 2011.

[4] Kılıç, Hakan, Neşet Sertaç Katal, and Ali Aydın Selçuk. "Evasion Techniques Efficiency Over The IPS/IDS Technology." In 2019 4th International Conference on Computer Science and Engineering (UBMK), pp. 542-547. IEEE, 2019.

[5] Rajan, Sriram Sundar, and Vijaya Krishna Cherukuri. "An overview of intrusion detection systems." Retrieved May 22 (2010).

[6] Prandl, Stefan, Mihai Lazarescu, and Duc-Son Pham. "A study of web application firewall solutions." In International Conference on Information Systems Security, pp. 501-510. Springer, Cham, 2015.

[7] Workman, Michael, William H. Bommer, and Detmar Straub. "Security lapses and the omission of information security measures: A threat control model and empirical test." Computers in human behavior 24, no. 6 (2008): 2799-2816.

[8] Kılıç, Hakan, Neşet Sertaç Katal, and Ali Aydın Selçuk. "Evasion Techniques Efficiency Over The IPS/IDS Technology." In 2019 4th International Conference on Computer Science and Engineering (UBMK), pp. 542-547. IEEE, 2019.

[9] Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, and Hafiz Khan. Dynamic & portable vulnerability assessment testbed with Linux containers to ensure the security of MongoDB in Singularity LXCs. In Companion Conference of the Supercomputing-2018 (SC18).

[10] Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, and Hafiz Khan. Vulnerability Prioritization, Root Cause Analysis, and Mitigation of Secure Data Analytic Framework Implemented with MongoDB on Singularity Linux Containers. In The 4th International Conference on Compute and Data Analysis -2020 (ICCDA-2020). San Jose, CA.

[11] Liao, Hung-Jen, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. "Intrusion detection system: A comprehensive review." Journal of Network and Computer Applications 36, no. 1 (2013): 16-24.

[12] Depren, Ozgur, Murat Topallar, Emin Anarim, and M. Kemal Ciliz. "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks." Expert systems with Applications 29, no. 4 (2005): 713-722.

[13] Huang, Yi-an, and Wenke Lee. "A cooperative intrusion detection system for ad hoc networks." In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 135-147. 2003.

[14] Mailewa, Akalanka and Jayantha Herath. "Operating Systems Learning Environment with VMware." In The Midwest Instruction and Computing Symposium. (MICS), Verona, WI, April 25-26 2014.

[15] Jin, Hai, Guofu Xiang, Deqing Zou, Song Wu, Feng Zhao, Min Li, and Weide Zheng. "A VMM-based intrusion prevention system in cloud computing environment." The Journal of Supercomputing 66, no. 3 (2013): 1133-1151.

[16] Stiawan, Deris, Abdul Hanan Abdullah, and Mohd Yazid Idris. "The trends of intrusion prevention system network." In 2010 2nd International Conference on Education Technology and Computer, vol. 4, pp. V4-217. IEEE, 2010.

[17] Simkhada, Emerald, Elisha Shrestha, Sujan Pandit, Upasana Sherchand, and Akalanka Mailewa Dissanayaka. "SECURITY THREATS/ATTACKS VIA BOTNETS AND BOTNET DETECTION & PREVENTION TECHNIQUES IN COMPUTER NETWORKS: A REVIEW, In The Midwest Instruction and Computing Symposium. (MICS), North Dakota State University, Fargo, ND, April 5-6 2019.

[18] Anderson, James P. "Computer security threat monitoring and surveillance, James P." Anderson Co., Fort Washington, PA (1980).

[19] Chakraborty, Nilotpal. "Intrusion detection system and intrusion prevention system: A comparative study." International Journal of Computing and Business Research (IJCBR) 4, no. 2 (2013): 1-8.

[20] ixiacom.com. (2020). IPS and IDS: Role and Function | Ixia. [online] Available at: https://www.ixiacom.com/company/blog/ips-and-ids-role-and-function [Accessed 1 Mar. 2020].

[21] Sperotto, Anna, Gregor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras, and Burkhard Stiller. "An overview of IP flow-based intrusion detection." IEEE communications surveys & tutorials 12, no. 3 (2010): 343-356.

[22] Li, Wan, and Shengfeng Tian. "Preprocessor of intrusion alerts correlation based on ontology." In 2009 WRI International Conference on Communications and Mobile Computing, vol. 3, pp. 460-464. IEEE, 2009.

[23] Sivaraman, Vijay, Hassan Habibi Gharakheili, Arun Vishwanath, Roksana Boreli, and Olivier Mehani. "Network-level security and privacy control for smart-home IoT devices." In 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 163-167. IEEE, 2015.

[24] Robert, Jean-Marc, and Francois JN Cosquer. "System and method for detecting abnormal traffic based on early notification." U.S. Patent 7,757,283, issued July 13, 2010.

[25] Lahoud, Hilmi A., and Xin Tang. "Information security labs in IDS/IPS for distance education." In Proceedings of the 7th conference on Information technology education, pp. 47-52. 2006.

[26] Bakar, Najwa Abu, Bahari Belaton, and Azman Samsudin. "False positives reduction via intrusion alert quality framework." In 2005 13th IEEE International Conference on Networks Jointly held with the 2005 IEEE 7th Malaysia International Conf on Communic, vol. 1, pp. 6-pp. IEEE, 2005.

[27] De Bruijn, Willem, Asia Slowinska, Kees Van Reeuwijk, Tomas Hruby, Li Xu, and Herbert Bos. "Safecard: a gigabit ips on the network card." In International Workshop on Recent Advances in Intrusion Detection, pp. 311-330. Springer, Berlin, Heidelberg, 2006.

[28] Borkar, Amol, Akshay Donode, and Anjali Kumari. "A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)." In 2017 International conference on inventive computing and informatics (ICICI), pp. 949-953. IEEE, 2017.

[29] Mailewa, Akalanka, Jayantha Herath, and Susantha Herath. "A Survey of Effective and Efficient Software Testing." In The Midwest Instruction and Computing Symposium. (MICS), Grand Forks, ND, April 10-11 2015.

[30] Sabahi, Farzad, and Ali Movaghar. "Intrusion detection: A survey." In 2008 Third International Conference on Systems and Networks Communications, pp. 23-26. IEEE, 2008.

[31] Ashoor, Asmaa Shaker, and Sharad Gore. "Difference between intrusion detection system (IDS) and intrusion prevention system (IPS)." In International Conference on Network Security and Applications, pp. 497-501. Springer, Berlin, Heidelberg, 2011.

[32] Roshan Ramprasad Shetty, Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, Ravi Vadapalli, and Hafiz Khan. 2017. Secure NoSQL Based Medical Data Processing and Retrieval: The Exposome Project. In Companion Proceedings of the10th International Conference on Utility and Cloud Computing (UCC '17 Companion). ACM, New York, NY, USA, 99-105.

[33] Onut, Iosif-Viorel, and Ali A. Ghorbani. "Features vs. attacks: A comprehensive feature selection model for network based intrusion detection systems." In International Conference on Information Security, pp. 19-36. Springer, Berlin, Heidelberg, 2007.

[34] Mitchell, Robert, and Ray Chen. "Behavior-rule based intrusion detection systems for safety critical smart grid applications." IEEE Transactions on Smart Grid 4, no. 3 (2013): 1254-1263.

[35] Keshri, Anand, Sukhpal Singh, Mayank Agarwal, and Sunit Kumar Nandiy. "DoS attacks prevention using IDS and data mining." In 2016 International Conference on Accessibility to Digital World (ICADW), pp. 87-92. IEEE, 2016.

[36] Chaturvedi, Palash, and Amit Saxena. "A Systematic Literature Survey on IDS." International Journal on Recent and Innovation Trends in Computing and Communication 5, no. 6: 671-676.

[37] Sandhu, Usman Asghar, Sajjad Haider, Salman Naseer, and Obaid Ullah Ateeb. "A survey of intrusion detection & prevention techniques." In 2011 International Conference on Information Communication and Management, IPCSIT, vol. 16, pp. 66-71. 2011.

[38] Roesch, Martin. "Snort: Lightweight intrusion detection for networks." Lisa. Vol. 99. No. 1. 1999.

[39] Timofte, Jack. "Intrusion detection using open source tools." Informatica Economica Journal Issn 14531305 (2008): 75-79.

[40] Anwar, Muhammad Masood, Muhmmad Faisal Zafar, and Zafar Ahmed. "A proposed preventive information security system." 2007 International Conference on Electrical Engineering. IEEE, 2007.

[41] Fekolkin, Roman. "Intrusion detection & prevention system: overview of snort & suricata." Internet Security, A7011N, Lulea University of Technology (2015): 1-4.

[42] Paxson, Vern, Jim Rothfuss, and Brian Tierney. "Bro quick start guide." Retrieved April 22 (2004): 2010.

[43] Resmi, A. M. "Intrusion Detection System Techniques and Tools: A Survey." (2017).

[44] Seagren, Eric. Secure your network for free. Elsevier, 2011.

[45] Jones, Blain R. "Network Security: An Open-Source Approach." (2005).