Intrusion Detection and Prevention Systems: An Updated Review

Chapter · January 2020

DOI: 10.1007/978-981-32-9949-8_48

6 authors, including:

Nureni Ayofe Azeez
University of Lagos
75 PUBLICATIONS **287** CITATIONS
SEE PROFILE

Taiwo Mayowa Bada
Bentley University
1 PUBLICATION **1** CITATION
SEE PROFILE

Sanjay Misra
Covenant University Ota Ogun State, Nigeria
485 PUBLICATIONS **2,421** CITATIONS
SEE PROFILE

Adewole Adewumi
Covenant University Ota Ogun State, Nigeria
76 PUBLICATIONS **203** CITATIONS
SEE PROFILE

Intrusion Detection and Prevention Systems: An Updated Review

Nureni Ayofe Azeez, Taiwo Mayowa Bada, Sanjay Misra, Adewole Adewumi, Charles Van der Vyver and Ravin Ahuja

Abstract The evolution of Information Technology (IT), cutting across several divides in our daily endeavors allows us to interact with all forms of data at different OSI model layers from application to physical. These data are susceptible to intrusion, aimed at compromising its integrity; thus, the need to protect these data, maintain its integrity, confidentiality, and availability cannot be overemphasized. Intrusion Detection and Prevention System (IDPS) is a device or software application designed to monitor a network or system. It detects vulnerabilities, reports malicious activities, and enacts preventive measures to keep up with the advancement of computer-related crimes using several response techniques. This paper presents an updated review on IDPSs given the fact that the most recent review found on the subject was done in 2016. It will also discuss the use of IDPSs to identify vulnerabilities in various channels through which data is accessed on a network or system and prevention mechanisms applied to mitigate against intrusion.

Keywords Vulnerabilities · Malicious activities · Prevention · Network · IDPS

N. A. Azeez · C. Van der Vyver
North-West University, Vaal Triangle Campus, Vanderbijlpark, South Africa
e-mail: nurayhn1@gmail.com

C. Van der Vyver
e-mail: charles.vandervyver@nwu.ac.za

T. M. Bada
University of Lagos, Lagos, Nigeria
e-mail: badataiwo@gmail.com

S. Misra (✉) · A. Adewumi
Covenant University, Ota, Nigeria
e-mail: Sanjaymisra@covenantuniversity.edy.ng

A. Adewumi
e-mail: wole.adewum@covenantuniversity.edy.ng

R. Ahuja
University of Delhi, New Delhi, India

N. Sharma et al. (eds.), *Data Management, Analytics and Innovation*, Advances in Intelligent Systems and Computing 1042, https://doi.org/10.1007/978-981-32-9949-8_48

1 Introduction

During 1984 and 1986, more research on intrusion detection system was done by several researchers. James P. Anderson's [1] presented a research on Intrusion Detection System (IDS). In the mid-1990s, IDS products were first commercialized by two companies, Internet Security System Inc (ISS) and Wheelgroup. They designed a network-based IDS called RealSecure and Netranger, respectively. ISS Inc. released the first version of RealSecure 1.0 for Windows NT 4.0. RealSecure used a knowledge base by matching signatures, however, it was ineffective for new attacks which became a major setback. Wheelgroup's Netranger was a known network-based IDS back in 1995; it functioned by scanning network traffic. Wheelgroup was acquired in by Cisco in February 1998; today, it forms an intrinsic part of Cisco's security.

Many researchers identified the setback in using the knowledge-based technique of matching signatures because it required continuous update of the database to recognize new attacks; more so, network and packet switching began to rise to a high speed from megabits to gigabits per sec. This was a major challenge as it became more difficult to scan through, analyze traffic, and detect attacks in real-time; thus, researchers were burdened with designing an IDS fit for high-speed networks. This led to the invention of host-based IDS, for example, TCP Wrappers, Tripwire, and Snort which provided analysis of system logs in real time. Snort is a free IDS tool, known for its multi-functionality as a network-based and host-based IDS. It was first released by Marty Roesch on December 22,1998 for UNIX systems; later in 1999, a version of Snort (version 1.5) was released; it was effective in analyzing and logging packets in real-time; it was later modified for Windows system by Michael Davis in the year 2000 [2].

Today, as the functionality of IDS advances, attackers now explore means of detecting, bypassing, and disabling IDS before penetrating the infrastructure, resulting in denial of service (DoS). Security experts aim to curb these attacks by using Intrusion Detection and Prevention System (IDPS) architectures which are not visible to attackers by restricting communication permitted among various security components on a network. Due to the gradually increasing number of vulnerabilities, the identification of attack is essential. To this end, a number of reviews have been done on IDPSs in the literature [3] with the most recent one being [4] which was conducted in 2016. A lot has happened since that period that is worthy of reporting. For instance, it was in 2016 that the biggest DDoS attacks powered by a Botnet [5] were recorded. An example is Mirai, a Botnet primarily composed of infected routers and security cameras, low-powered and poorly secured devices which caused a lot of major DDoS attacks [6].

Internet attacks thus must be defined to measure security. Also, in recent times, infrastructure has evolved from a network of systems, private cloud infrastructure to the Internet of Things (IoT) offering several cloud-based services and solutions. While this has provided limitless opportunities on the choice of where to store data, the risk that accompanies these opportunities is also considered enormous because

these data can be compromised via several intrusion methods irrespective of the platform on which the data is stored [7].

2 Motivation

Intrusion is a criminal act committed against an information system, e.g., computer system, network or web infrastructure, such that security on the system is breached or compromised thereby putting it in an insecure state which allows for unauthorized access to the data being hosted by the system. This is done either by bypassing, disabling or exploring vulnerabilities on the system, typically leaving traces which can be discovered by the intrusion detection system.

The most recent review [4] focused majorly on network intrusion detection systems. The elements of security here are basically availability, accuracy, access control, confidentiality, integrity, and identification [8]. Intrusive attacks can be classified into passive [9] and active [5] attacks. An attack is classified as active when data is being altered with the intent to corrupt, destroy the data or the entire network hosting the data [5, 10]. An example of an active attack is interruption. This can include Denial of Service (DoS) [9], Distributed Denial of Service (DDoS) [6], SQL Injection [11], fabrication, replay attack [9], masquerading [12], and modification [5]. Some examples of passive attacks include traffic analysis [9], sniffing [5], and keyloggers [13]. The drawback of the study includes the fact that it mentioned but did not show the classification of intrusion detection systems. Also, network IDPS are known to identify abnormal behavior in network nodes only after the damage has been done to network resources [14]. Furthermore, with the increasing growth of the Web—a global network—network intrusion detection systems are limited in capacity at detecting anomalies on the web.

Newer models comprising a combination of machine learning techniques are being applied to combat attacks on the Web [15]. Some of the models also respond to security threats by detecting various malware intrusions and protocol authentication based on human behavior.

In addition, IDPSs are also being developed for cloud-based environments/systems; hence, the deployment of distributed IDPSs in cloud systems raises many challenges due to the diversity of its services and the complexity of its infrastructure.

3 Intrusion Detection and Prevention Systems

Security systems are designed in practice, to detect, identify and respond to malicious attacks against, a computing system, network or in general, information systems. These attacks are aimed at undermining the integrity of these systems,

steal information and in some cases cause damage to the systems thereby making the system unavailable.

IDS is either a software or hardware that automates intrusion detection, monitors network traffic for suspicious activities, and sends notifications to an administrator [7]. Intrusion Prevention System (IPS) is a software or hardware that prevents an intruder from gaining access to a network, let alone attack a network [16].

Today, security experts are trending with security appliance combining both intrusion detection and prevention capabilities which identify, log possible incidents, prevent attack, and send report to an administrator [16, 17]. Intrusion Detection and Prevention Systems (IDPS) ensures that the protection, availability, integrity, and confidentiality of information systems are guaranteed.

IDPS has become important when putting the security of information systems into context, preserving data, protecting data from unauthorized access or theft, and ensuring continuous availability of services that these information systems provide. Until recently, attackers' focus was on bank customers, where accounts were raided through fraudulent acquisition of personal details either by sending phishing emails or keyloggers, and credit cards were stolen [18].

3.1 Classification of Intrusion Detection and Prevention Systems

IDPS can be classified based on the following criteria [19]:

1. **Type of Intruder**: This is either external or internal. An external intruder is one who does not have any form of access to a network or service, while an internal extruder is one who has authorized access to a network but has restricted permissions on the network.
2. **Type of Intrusion**: There are various types of intrusions which are discussed in chapter two.
3. **Detection Technique**: Three different types of techniques are normally adopted for intrusion detection, misuse detection, anomaly detection, and stateful protocol analysis [20].

    - **Misuse Detection**: It is a signature-based detection method which matches intruder attack patterns, represented by signatures against a knowledge base of known exploit on software and system vulnerabilities. Signature-based detection analyzes and identifies specific patterns of events or behavior that portray an attack using either static, dynamic or hybrid approach. The static approach in misuse detection analyzes intrusion activities against a program and its code before execution. Dynamic approach analyzes attack patterns during or after the execution of a program while hybrid combines both static and dynamic approach to detect malicious attacks [21].

- **Anomaly-Based Detection**: It is a behaviur-based detection technique which gets its input from audit logs generated from the operating system. This type of technique looks for variations in behavior which might indicate masquerading. Anomaly-based detection uses profiles created through monitoring the behavior of typical activity or models of intended behavior of users and applications over a period. It analyzes malicious attacks by using these profiles which represent the normal behavior of users, hosts, network connections, or applications against profiles of monitored activities; any deviation from the norm is triggered via an alert system [21].
- **Stateful Protocol Analysis**: Stateful [22] protocol analysis detects changes of protocol state. Unlike the anomaly detection method, this adopts predetermined universal profiles created based on accepted definitions of protocol behavior created by vendors and industry leaders [23].
- **Rule-based**: This involves making decisions based on rule sets which are defined by domain experts. They can detect known attacks but are incapable of detecting novel attacks. Also, with increase in network traffic, finding and coding rule sets is both difficult and time-consuming.
- **Supervised Machine Learning (ML)**: It does not require model building as in the case of anomaly-based detection. Rather it is able to learn complex malicious and normal models.
- **Unsupervised Machine Learning**: An example is clustering-based IDPS. This approach to intrusion detection involves building models with unlabeled data; however, their performance is not as good as the supervised models (Table 1).

3.2 Types of Intrusion Detection and Prevention Systems (IDPS)

IDPS will be discussed based on the way they are deployed and the type of activities they monitor [16].

- Network-Based Intrusion Detection and Prevention System (NIDPS)
- Wireless Intrusion Detection and Prevention System (WIDPS)
- Network Behavior Analysis (NBA)
- Host-Based Intrusion Detection and Prevention System (HIDPS)

3.2.1 Network-Based IDPS

Network-Based IDPS (NIDPS) technology is designed to analyze packets at the network, transport, and application layer of the Open System Interconnection (OSI) model. NIDPS is most efficient when deployed within a network

Table 1 Advantages and disadvantages of intrusion detection techniques

Detection techniques	Advantages	Disadvantages
Signature-based detection	Effective and simple method of detecting known attacks since it uses signatures of known attacks	Cannot track unknown attacks and variants of known attacks
	Analyzes and identifies attacks by matching malicious signatures against known knowledge base	Attackers can make adjustment to attacks to avoid matching known attack signature
	Detection accuracy for known attacks is high	Requires continuous update of signatures or patterns
	Low computational cost	Newer attack signatures may not be in the signature database
	Rate of false alarm is very low	Detect only the attacks for which they are configured
Anomaly-based detection	Ability to detect and reduce the false alarm rate of unknown attacks	Detection accuracy is based on the amount of collected behavior or features
	Can detect new and unforeseen vulnerabilities	Well-known attacks may not be detected if they fit established a profile
	Dependency on the operating system is minimal and it is able to detect privilege abuse	Intruder can change profile slowly over a period
	Uses statistical test on collected behavior to identify intrusion	Configuring profiles is time-consuming
	No need for priori knowledge of security flaws	Less effective in the dynamic environment due to constant changes in monitored events
	System can also detect attacks from inside a network	
Stateful analysis	Adds stateful characteristics to regular protocol analysis	Resource intensive for protocol state tracing and analysis
	Distinguishes unexpected sequences of commands	Cannot detect attacks that do not violate the characteristics of generally accepted protocol behavior
	Identifies unexpected sequences of commands	
Rule-based	Can easily detect known attacks	Unable to detect unknown attacks
		Finding and coding rule sets is both difficult and time wasting
Supervised ML	Ability to learn complex and malicious models	They are hardly ever used in a real-world scenario owing to the fact that they require sufficient supply of labeled branding data
		Training data is labeled by domain experts which is both costly and time-consuming
Unsupervised ML	Works with unlabeled data on domain specialist may not be required	Performance is not as good as supervised ML

infrastructure with a specific design where it is able to monitor and analyze real-time packets for intrusion and take a decision on any suspicious activity. While NIDPS is effective in analyzing and detecting suspicious network packets in real time, it cannot analyze encrypted traffic, traffic over Virtual Private Network connection (VPN), SSH or HTTPS sessions, and traffic on mobile computing networks [17].

NIDPS has broad intrusion detection capabilities. An example of an NIDPS is KEMP Loadmaster which can detect intrusion and prevent intrusion by shutting down the device.

3.2.2 Wireless IDPS

WIDPS is a variant of NIDPS which monitors and analyzes packets and protocols on a wireless network. Despite its ability to analyze network traffic, WIDPS cannot detect abnormal activities within an application [17].

Advantages

- It is effective for monitoring and analyzing intrusion on a wireless network.
- WIDPS can identify various problematic issues like policy violations and mis-configurations at the WLAN protocol level.

Disadvantages

- It is vulnerable to DoS attacks.
- It cannot monitor and analyze packets on transport layer, network layer, and application layer.
- It is susceptible to evasion technique when an intruder attacks channels that are not currently monitored.

3.2.3 Network Behavior Analysis (NBA)

NBA is also a variant of NIDPS with the ability to monitor and analyze network traffic to detect unusual activities that may emanate from violation of policy, DDoS attacks or malware intrusion [17].

Advantages

- It is effective in detecting DoS attacks.
- It is effective for monitoring packets on transport, network application TCP/IP layer, etc.
- It can monitor and detect threats caused by malware, policy violation, and DDoS.

Disadvantages

- Packets are analyzed in batches, thus delaying the rate of intrusion detection.

3.2.4 Host-Based IDPS

Host-Based IDPS technology is designed for Application level and Operating System intrusion detection and prevention by monitoring the events on a single host on which it is installed. Aside from having the capability of monitoring and analyzing network traffic, HIDPS can analyze system-specific settings such as software calls, local security policy, and audits logs within the host for suspicious activities. HIDPS functionality can be divided into four categories [17]:

- **File System Monitoring**: Every system has a file system to detect and prevent intrusion; HIDPS monitors file systems regularly by checking variations in files size and file content against a known knowledge base. Whenever a system or user file shows a significant deviation, an alert is triggered which sends a notification to an administrator, indicating the detected intrusion and the action taken to prevent access or damage to the file [23].
- **Log File Analysis**: System events are generally logged in a file. These files (event logs) are analyzed constantly by HIDPS for changes or abnormal activities; a typical event log changes in the login information.
- **Connection Analysis**: HIDPS monitors and analyzes network packets (TCP/IP) for suspicious activities such as the ratio or sequence of TCP/IP connections on the host on which it is installed [24].
- **Kernel-Based HIDPS**: The kernel is provided with extra security capability which allows it to identify and prevent intruder activities itself.

Advantages

- It can detect intrusions on host applications, operating system, and network layer traffic.
- It can monitor and analyze suspicious activity on encrypted communication.
- It can detect intrusion on host systems by monitoring its file system, file access, system calls, etc.
- It does not require additional hardware since it is deployed on the host system.
- It can detect misuse of profile because it interacts with the user, as well as server installed application.
- It can prevent intrusion at the system level and detect attacks which NIDPS cannot detect.

Disadvantages

- It does not use a predefined database, therefore, detection accuracy is limited.
- Its uses more host resources, therefore, impacting on the system host performance.
- It must be deployed on each host which is expected to monitor.
- Its monitoring is restricted to the host on which it is deployed.
- There is a possibility of conflict with preexisting security configuration.

4 IDPS, Design, and Architecture

Information systems today have become a target for hackers whose only aim is to undermine the integrity, availability, and confidentiality of data. Therefore, proper design consideration must be put in place when designing an IDPS to increase its capacity to detect a threat and prevent it from gaining access to an information system. In designing an IDPS, the following must be considered [25].

4.1 Speed and Accuracy

These are highly desirable features. The sensitivity of an IDPS in terms of its speed and accuracy determines the rate of false negatives and false positives reported by the system. If the sensitivity of an IDPS is too low, it will have a high rate of false negative where intrusive activities are not detected, thus, no alert is triggered. Whereas if the sensitivity of an IDPS is too high, there is a high tendency of reporting false positives where an alarm is triggered for nonintrusive activities. False negatives and false positives can be triggered by several factors discussed below [26].

Causes of False-Negative Alerts:

- Improper spanning of switch ports which can cause network traffic to overwhelm the switch which can contribute to events with false-negative triggers.
- Flaws in the design of encrypted traffic which are usually not clear to the IDPS.
- A poorly written signature which does not have the capacity to detect an attack even though the attack is known.
- Improper communication of change management on network and server infrastructure to the information security team.
- Intrusive attacks caused by unpublicized or new attacks thus making it invisible to existing signatures.

Causes of False-Positive Alerts:

- A reactionary traffic alarm caused by equipment failure can trigger a false positive alert. For example, an ICMP flood caused by unreachable destination can trigger a false positive alert.
- An equipment-related alarm, e.g., a load balancer can trigger an alert generated from unrecognized packets from the equipment itself.
- A poorly written client software can trigger alerts of policy violation, e.g., alerts triggered by software bugs.
- Alerts triggered by unmalicious events.

4.2 Logging Capabilities

The logging capability of an IDPS is also very important because it facilitates its ability, identifies, detects, and reports malicious activities. The following are the logging capabilities to consider when designing an IDPS:

- IDPS must be able to log time stamps which include the date and time the malicious activity occurred.
- IDPS must be able to log connection ID, usually a unique number assigned to a session or a TCP connection.
- IDPS must effectively log an alarm type, set its severity rating, impact, and the priority of attack.
- IDPS must have the capacity to analyze protocols like TCP, UDP, ICMP at the network, application, and transport layer.
- IDPS must be able to identify the source and destination IP of connections and determine the number of bytes transmitted over the connection.
- IDPS must effectively understand the characteristics of application request and responses.

4.3 Information Gathering Capabilities

For an IDPS to be effective in detecting and preventing malicious activities on an information system, it must be able to gather information about the system upon which it is deployed.

- IDPS must be able to gather information on host profiles which include host IP and their corresponding MAC address.
- Ability to determine the OS version to enable it to determine the type of vulnerability it is susceptible to.
- Ability to identify network characteristic by gathering information on changes in network configuration.

4.4 Architecture of IDPS

Depending on the expected outcome, IDPS can be deployed using the following architecture [20]:

- Centralized: This architecture collects data centrally, sends it to a single location for analysis. Data collection is either from a single host or from several hosts.

- Hierarchical: This architecture collects data from several hosts which are analyzed according to the layers of the deployed IDPS.
- Distributed: This architecture collects data host by host and it is analyzed.

5 Conclusion

Security threats and incidents have evolved and pose a great challenge to information systems; thus, the importance of deploying an IDPS cannot be overemphasized and efforts to create more security techniques must continue to ensure that the integrity, originality, and confidentiality of information systems is guaranteed, thus making it accessible to everyone when the need arises.

IDPS in its various forms according to Chap. 3 is essentially beneficial in that it has the capacity to identify and detect vulnerabilities and prevent all forms of intrusion discussed in Chap. 2. However, consideration must be given to the type of deployment method to get the best of IDPS.

Furthermore, IDPS has extensive logging capacity which makes it effective in intrusion detection, most especially against signatures of various attacks against network systems; this has made a necessity for enterprise environment to protect data, as data sharing of all sorts has evolved to a global trend.

Lastly, when multiple IDPS technologies are combined into a single protection solution, it reduces management costs considerably because IDPS engages several techniques in intrusion detection and prevention; thus when developing a security strategy, it is important that it is comprehensive to stay ahead of the next threat.

References

1. Anderson, J.P.: Computer Security Planning Study. Washington (1972). Retrieved from https://pdfs.semanticscholar.org/0735/6c5477c83773bd062b525f45c433e5b044e8.pdf
2. Bruneau, G.: The History and Evolution of Intrusion Detection, vol. 7 (2001). Retrieved from https://www.sans.org/reading-room/whitepapers/detection/history-evolution-intrusion-detection-344
3. Patel, A., Taghavi, M., Bakhtiyari, K., Júnior, J.C.: An intrusion detection and prevention system in cloud computing: a systematic review. J. Netw. Comput. Appl. **36**, 25–41 (2013)
4. Amudhavel, J., Brindha, V., Anantharaj, B., Karthikeyan, P., Bhuvaneswari, B., Vasanthi, M., Nivetha, D., Vinodha, D.: A survey on intrusion detection system: State of the art review. Indian J. Sci. Technol. **9**, 1–9 (2016)
5. Ahmad, K., Verma, S., Kumar, N., Shekhar, J.: Classification of internet security attacks. In: Proceedings of the 5th National Conference; INDIACom-2011. New Delhi (2011). Retrieved from https://www.researchgate.net/publication/262494946_Classification_of_Internet_Security_Atta
6. Symantec.: Internet Security Threat Report. Mountain View, CA 94043 (2017). Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
7. Kemmerer, R.A., Vigna, G.: Intrusion detection: a brief history and overview, pp. 27–29 (2002). Retrieved from https://www.computer.org/csdl/mags/co/2002/04/r4s27.pdf

8. Persa, S.: Network Security (2003). Retrieved from https://utcluj.ro/pub/docs/cursuri/prc_eng/stallings/securitarea.ppt
9. Pawar, M.V., Anuradha, J.: Network Security and Types of Attacks in Network, pp. 504–506 (2015). Retrieved from https://ac.els-cdn.com/S1877050915006353/1-s2.0-S1877050915006353-main.pdf?_tid=84c3d323-6ab4-4ca1-86f5-7eafc2cbfb30&acdnat=1530640171_af15fb42c5d503b379a7da902477f68d
10. Bloomberg, J.: Cybersecurity Lessons Learned From 'Panama Papers' Breach. The Little Black Book of Billonaire Secrets (2016). Retrieved from https://www.forbes.com/sites/jasonbloomberg/2016/04/21/cybersecurity-lessons-learned-from-panama-papers-breach/#453217b12003
11. Clarke, J.: SQL Injection Attacks and Defense, 2nd edn. Elsevier, Waltham (2012)
12. Salem, M.B., Stolfo, S.J.: Data collection and analysis for masquerade attack detection: challenges and lesson learned. Columbia University, Computer Science. New York: Department of Computer Science, Columbia University (2011). Retrieved from https://doi.org/10.7916/D8D50VV1
13. Wood, C.A., Raj, R.K.: Keyloggers in Cybersecurity Education. New York: Rochester Institute of Technology (2010). Retrieved from https://pdfs.semanticscholar.org/d1d4/628a22e8d27c6cd202839d7bf0e3a7c7ea91.pdf
14. Yerur, S.V., Natarajan, P., Rangaswamy, T.R.: Proactive hybrid intrusion prevention system for mobile adhoc networks. Int. J. Intell. Eng. Syst. **10**, 273–283 (2017)
15. Johnson Singh, K., Thongam, K., De, T.: Entropy-based application layer DDoS attack detection using artificial neural networks. Entropy **18**, 1–17 (2016)
16. Chee, J.: Host Intrusion Prevention Systems and Beyond, vol. 26 (2008). Retrieved from https://www.sans.org/reading-room/whitepapers/intrusion/host-intrusion-prevention-systems-32824
17. Letou, K., Devi, D., Singh, J.Y.: Host-based intrusion detection and prevention. Int. J. Comput. Appl. **0975–8887**(69), 27–32 (2013)
18. NSS Labs.: Security Value Map. Next Generation Firewall (NGFW), p. 1 (2017). Retrieved from https://www.nsslabs.com/research-advisory/security-value-maps/2017/ngfw-svm-graphic/
19. Santos, K.B., Chandra, S.T., Phani, R., Ratnakar, M., Baba, D.S., Sudhakar, N.: Intrusion detection system- types and prevention. Int. J. Comput. Sci. Inf. Technol. 77–82 (2013). Retrieved from http://ijcsit.com/docs/Volume%204/Vol4Issue1/ijcsit2013040119.pdf
20. Singh, A.P., Singh, M.D.: Analysis of host-based and network-based intrusion detection system. Comput. Netw. Inf. Secur. 41–47 (2014). Retrieved from http://www.mecs-press.org/ijcnis/ijcnis-v6-n8/IJCNIS-V6-N8-6.pdf
21. Ghafir, I., Husak, M., Prenosil, V.: A survey on intrusion detection and prevention (2014)
22. Williams, T., Shirley, M.: Next Generation Intrusion Prevention System (NGIPS) Test Report. NSS Labs (2017). Retrieved from https://www.forcepoint.com/resources/reports/nss-labs-2017-next-gen-ips-report
23. Masaryk University, Faculty of Informatics. Brno, Czech Republic: Researchgate. Retrieved from https://www.researchgate.net/profile/Ibrahim_Ghafir/publication/305957314_A_Survey_on_Intrusion_Detection_and_Prevention_Systems/links/57a75a2708aefe6167bc1de0/A-Survey-on-Intrusion-Detection-and-Prevention-Systems.pdf?origin=publication_detail
24. Scarfone, K., Mell, P.: Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology Special Publication 800-94, 127 (2007). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf
25. Sharifi, A., Zad, F.F., Noorollahi, A., Sharifi, J.: An overview of intrusion detection and prevention systems (IDPS) and security issues. IOSR J. Comput. Eng. (1OSR-JCE) **16**(1), 47–52 (2014)
26. Stawowski, M.: The Principles and Good Practices for Intrusion Prevention Systems Design, vol. 25 (2006). Retrieved from https://pdfs.semanticscholar.org/8cac/01d90c44ae710719df662f858ca17ffc96d1.pdf