International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I3P204
Volume 69 Issue 3, 17-22, March 2021

Counteraction Against Digital Data Leak: Open Source Software for Intrusion Detection and Prevention

Nguyen Huy Binh[1*], Le Trung Kien[2]

[1,2]*People's Police Academy, Hanoi, Vietnam*

Abstract: *This work performs a generalized analysis of intrusion detection systems (IDS) software in terms of a certain basic set of criteria. The IDS are studied, their essence is specified and disclosed comprehensively. Publications devoted to the analysis of software for detection and prevention of cyber threats and intrusions are reviewed. On the basis of the experimental results, six modern IDS are analyzed in terms of nine basic criteria: Class of cyberattacks, Adaptivity, Methods of detection, System control, Scalability, Surveillance level, Response to cyber attack, Security, and OS support. It has been concluded that the analysis of software for intrusion detection by basic criteria allows developers and users to select open-source software for information systems protection.*

Keywords: *administering, software, cyber attack.*

I. INTRODUCTION

The intensive development of information systems (IS) and technologies comprehensively influences all spheres of society's activities. A significant number of modern governmental and private companies use IS for management of production processes, support to decision making, searching for required data, etc. This provides numerous advantages related to labor efficiency and mobility of employees, high rate of access to information and services, opportunities for remote control of resources and process, etc.

Meanwhile, the number of vulnerabilities and threats to IS increases; hence, in order to provide their normal operation and to prevent intrusions, specialized security means are required. It should be mentioned that one of the relevant trends, which is being intensively developed in the spere of information security, is the detection of cyber attacks and prevention of intrusions in IS by unauthorized source (UAS). In addition, it should be mentioned that attacks on IS resources (ISR) become more and more perfect, more global, and more frequent.

Massive cyberattacks initiate the development of specialized engineering solutions, means, and systems of counteraction. Networks intrusions are detected by modern methods, models, means, software, and integrated solutions for intrusion detection and prevention systems [1], which could retain their efficiency upon the occurrence of new or modified cyber threats. However, in practice, upon the occurrence of new threats and abnormalities generated by attacking actions with undefined or ill-defined properties, the mentioned means are not always efficient and require long-term resources for their respective adaptation. Therefore, the intrusion detection systems (IDS) should be continuously analyzed and improved in order to provide their continuous efficiency [2], [3].

Among such systems, there is specialized software aimed at detecting suspicious activity or intrusion in IS accompanied by adequate measures to prevent cyber attacks. These systems and means, as a rule, are sufficiently expensive, based on closed source code, and require periodical support by developers (qualified experts), aimed at their improvement and appropriate adjustment for conditions of specific companies [4].

Therefore, analysis of engineering solutions, specialized means, and software of cyber-attack detection, abuses, and abnormalities in IS for their application upon selection and development of IDS, as well as the determination of the most efficient mechanisms of ISR protection, are an urgent task.

II. LITERATURE REVIEW

Numerous scientific publications are devoted to the analysis of software for the detection and prevention of cyber threats and intrusions (Table 1).

TABLE I. ANALYSIS OF IDS

Reference	Field of application
[5]	General description of some functions and operation principles of various IDS
[6]	Main operation principles of the most popular IDS and respective supporting OS
[7]	Host and network IDS are compared
[8]	Functionality and performance of various IDS are estimated
[9]	IDS types are analyzed regarding the opportunity of monitoring, types of notifications, and warnings about attack and adjustments options
[10]	Open source IDS are analyzed and compared in terms of some properties regarding the best application of IS protection

[11]	Methods used for the detection of attacks and abnormalities are described
[12]	IDS composition and their main tasks are disclosed
[13]	Methods and models used for intrusion detection are described
[14]	Methods of detection of attacks and abnormalities are compared
[15]	IDS classification is proposed, their advantages and disadvantages are mentioned, as well as certain principles of their design
[16]	The main opportunities, design concepts, operation mechanisms of IDS are described
[17]	IDS designing is analyzed, main principles of their development are demonstrated

It has been determined that for modern IS and networks, there exists an urgent issue of rapid detection of abuses and abnormalities. However, most of the mentioned publications provide only partial analysis of IDS and their classification; a general description of respective support is given, which does not contain the required set of properties for integrated estimation of such systems.

Therefore, this work is aimed at the generalized analysis of IDS software using a predetermined basic set of criteria. This would provide certain opportunities to select such means and to develop the most efficient security mechanisms in the case of cyberattacks.

The research hypothesis is as follows: analysis of software for intrusion detection by basic criteria makes it possible to select open-source software for IS protection.

The research objectives include:

- determining basic criteria for modern IDS estimation;
- analyzing modern IDS according to the basic criteria.

This article is comprised of the following sections: Introduction, Literature review, Methods, Results and discussion, and Conclusion.

III. METHODS

Taking into account the known results with their subsequent generalization and reflection onto an expanded range of software for detection of abuses and abnormalities, six IDS were analyzed in terms of nine basic criteria: Class of cyberattacks, Adaptivity, Methods of detection, System control, Scalability, Surveillance level, Response to cyber attack, Security, and OS support.

At first, let us define each of the basic criteria.

Class of cyber attacks: determines the ability of the system to detect abnormalities and abuses at various IS levels. Most modern means are capable of detecting both classes of attacks (abnormalities and abuses).

Abuses are based on the use of existing drawbacks of IS. The main difference between abnormality and abuse is that abnormality is a process initiated before possible intrusion into the system or indicates an already existing attack. In fact, the abnormality is a deviation from the system's normal state, unusual activity, which can evidence certain attacking actions.

Adaptivity: allows the system to efficiently adapt to new attacks (unavailable in signature base) and to detect cyber attacks with minor modifications.

Methods of detection: numerous methods used for detection of attacks and comprising mathematical base of the system. The most popular are the methods of statistical and cluster analysis, management of event changes, attack graphs, signature, dynamic, machine learning, behavioral, heuristic, expert, fuzzy sets, etc.

System control: determines the scheme of control and its level. The control can be performed centrally from a single host or distributed from single hosts related by one system. Centralized systems control all means (modules) of intrusion detection from one station, and distributed systems implement control separately, where each module is responsible for its function.

Scalability: the possibility to expand the system.

Surveillance level: the system level at which data are acquired for the detection of cyberattacks. Two levels of data acquisition are applied: network and system. Modern systems, as a rule, support both surveillance levels since their interaction provides the best protection. This property determines the rate of formation of primary data, their correct processing, and obtaining accurate information about the current state of ISR.

Response to cyber attack: determines the existence of components or modules of counteraction in the system. That is, after attack detection, the actions are initiated aimed at reduction of further negative influence.

Security: characterizes availability of own system components responsible for its protection against cyber attacks and external negative data impact as well as for failure resistance and decrease in project vulnerability as a whole.

OS support: characterizes OS type, which supports respective software.

IV. RESULTS

On the basis of the proposed criteria, the properties of respective IDS are disclosed (see Table 2).

TABLE II. IDS ANALYSIS

No.	IDS	Classes of cyber attacks		Adaptivity	Methods of detection										
		Abuses	Abnormalities		Expert	Statistical	Signature	Scenario graphs	Event change control	Cluster	Dynamic	Machine learning	Behavioral	Heuristic	Fuzzy sets
1	AAFID	+	+	-	+	-	+	-	-	-	-	-	-	-	-
2	NetSTAT	+	+	+	-	-	+	-	+	-	-	-	-	-	-
3	ASAX	+	-	-	+	-	-	-	-	-	-	-	-	-	-
4	OSSEC	+	+	-	-	-	+	-	-	-	-	-	-	-	-
5	Suricata	+	+	+	-	+	+	-	-	-	-	-	-	-	-
6	Samhain	+	+	+	-	+	-	-	-	-	+	-	+	-	-

TABLE II. IDS ANALYSIS (CONTINUED)

No.	IDS	System control		Scalability	Surveillance level		Response to cyber attack	Security	OS support			
		Centralized	Distributed		System	Network			Unix	Linux	Windows	MacOS
1	AAFID	+	-	+	+	-	-	-	+	+	-	-
2	NetSTAT	-	+	+	+	+	+	+	+	+	-	-
3	ASAX	+	-	+	+	-	-	-	+	+	-	-
4	OSSEC	+	+	+	+	-	+	+	+	+	+	+
5	Suricata	+	-	+	-	+	+	-	+	+	+	+
6	Samhain	+	+	+	+	-	+	+	+	+	+	+

V. DISCUSSION

Then, let us consider the analyzed IDS in more detail.

AAFID. AAFID (USA) is intended for distributed control and detection of intrusions. It uses small autonomous programs (agents) to perform monitoring in network hosts. The AAFID architecture is based on independent simultaneously working objects (agents) aimed at the detection of intrusions. They control a certain set of system properties and inform about nonstandard behavior or specified events. The information obtained by the agents is integrated at the level of the main computer, where the events (obtained from different agents), which can be caused by one and the same attack, are correlated. Moreover, the reports from each computer are aggregated at a higher level (network level), thus allowing to detect cyberattacks from various sources [18].

This software processes only registration logs of software and OS where it operates. Information from each agent or host (set of hosts) is acquired in AAFID by means of hierarchical structure. Therefore, any suspicious activity in the network is detected, though the mentioned property does not always operate efficiently, since the system capabilities depend on the quality and quantity of available agents (programs), which are used for detection of these or those attacks [19].

The mentioned software uses expert and signature methods for the detection of abnormalities and abuses in network traffic, and it has centralized control from the main monitor. Due to the hierarchical structure of the system, AAFID can be easily modified. The system has an open interface for the addition of new agents and filters, which allows simple scaling and adaptation to network needs [19].

It should be mentioned that AAFID does not contain special mechanisms of protection and response to

intrusions; it is not resistant against cyber attacks, which are aimed at it.

NetSTAT. NetSTAT (USA) is based on extensible state/transition-based attack description language (STATL). The basic language uses the most abstract notions and does not depend on a specific system and its configuration. The language allows to supplement it, it is extensible; and by adding specific for certain system events, it can be easily adapted to various targeted environments. Intrusion is described as a consequence of actions for each new event. Such description is grouped into the module of language expansion, and it can be used in the description of cyber-attack scenarios for NetSTAT [20].

The system has two operation modes. The first one is based on the fact that for each state, the property of security and the transitions upon changes in the system state are determined. The attacks are described in the form of consecutive transitions. The second one is based on the signature approach, that is, on the description of attacks in the form of a sequence of transitions and templates, with which comparison is made to detect intrusions in a network environment. NetSTAT is oriented at operation in real-time mode [20].

The method of registration of state transitions partially allows the identification of new abnormality or attack but does not completely solve the issue of system adaptivity. This is an open-source project which allows designing scalable IDS on the basis of corporate targets.

The NetSTAT operation is based on the method describing the protected system in the form of states of its components with subsequent analysis of their transitions as a consequence of external impacts. When necessary, the transitions are recorded in logs of event registration, facilitating further detection of abnormalities or abuses in the system. The control is distributed since the system has a branched and complicated structure. The NetSTAT architecture allows to development of agents or sensors aimed at the detection of attacks or abuses at different levels of the network or system. System surveillance is carried out at system and network levels. In addition, NetSTAT can detect points and network events, which should be controlled [20].

ASAX. ASAX (Belgium) is a universal expert system for intrusion detection. Its operation principle is based on the description of the initial system in the form of a set of states with their subsequent analysis. ASAX is supported by a simple language: RUSSEL, which uses special rules for efficient processing of consecutive big files based on analysis of registration logs. RUSSEL can be considered as a procedural language including a specific predetermined structure of management, which is suitable for substantiation of recording sequence. This management structure is based on a specific mechanism initiating the rule containing a description of its activation condition and subsequent actions (for instance, output, message, or calling another rule). The main rule is the base of all sets, which is activated first, then the rules in the field of its action are called. In addition, it is possible to use the system for processing registration logs in real-time [21].

ASAX is based on a simple variant of the implementation of expert IDS. It has an open interface and program code, which allows the expansion of functional abilities. This software can be controlled centrally on the node of its installation by means of configuration files. Simple scaling is stipulated by the simple structure of ASAX. Since the system operates only with registration logs of applications and OS, it is characterized by system surveillance [21].

OSSEC. OSSEC (USA) is a scalable multiplatform link IDS based on the host with open-source input code [22]. It has the powerful tool of correlation and integrated analysis of logs, file integrity checking, Windows registry monitoring, centralized policy surveillance, rootkit detection, notification about attacks in real-time, bookmarks detection, and counteraction against intrusion [22].

In the case of intrusions, using respective logs sent to e-mail, it is possible to know about attacks and to apply the necessary measures. In addition, OSSEC can export notifications to any SIEM system by means of a system log. This facilitates obtaining analytical materials in real-time, reviewing and analyzing events in the security system [23].

The system uses agents (a set of small programs installed in the system for monitoring), which acquire information and send it to the manager for analysis and correlation. Part of the information is acquired in real-time, and another part – at preset intervals. OSSEC can be installed on the Microsoft Windows platform and act as an agent. The system is used by internet providers, universities, and big corporate centers of data processing [23].

Suricata. Suricata (USA) is open-source software, and it is a free, rapid, reliable, and promising tool for the detection of network threats. It is intended for the prevention and detection of intrusions in real-time, network security monitoring, automatic analysis, and PCAP file processing [24].

In addition, it is possible to detect attempts or intrusions, which are hidden by usual requests; there is the function of file removal for their checking. Suricata architecture facilitates the optimum distribution of computing among several processor cores. For instance, if video adapters are mostly idle, then they can be partially loaded with certain computations [24].

This software can detect intrusions in real-time, prevent intrusions into the system, inspect the properties of network security and combine detection of abnormalities and abuses. Moreover, Suricata can be adapted to new attacks, can control network traffic, and has powerful support of scenarios for the detection of complex threats [24].

In Suricata, the response to cyber-attack is performed rapidly if at least one of the predefined rules is activated by marking the obtained data packages by one of three markers: NF_ACCESS (access allowed); NF_DROP (access prohibited); NF_REPEAT (packages are marked and resent to rules of firewall which decides further assignment of respective packages) [24].

Samhain. Samhain (Germany) is an open-source, free, multiplatform software for IDS. It is also known as a host system that provides checking of files, review and analysis of logs, detection of malicious code, hidden applications, and processes, etc. [25].

Samhain is developed as a monitor for numerous hosts with various OS and for local PCs. One of its functions is a stealth mode, which allows hiding against UAS. In addition, in order to prevent intrusions, Samhain protects its central logs and configuration backups. The software can work in real-time, perform system files and logs checking, detect hidden software as well as malicious programs and abnormalities [25].

Samhain is loaded as a system daemon (service) and silently detects threats. The stealth mode allows the system to be invisible for malicious software; hence, UAS will not counteract respective monitoring without preliminary information about it. Due to such a mode, Samhain is able to terminate or reload processes, which allows detecting possible threats. This software is more intended for server applications and can inspect connection with server and identification of correct password upon logging in [25].

Counteraction to attacks in Samhain is carried out at three levels:

- the first is based on inspection of checksums (cryptographic checksums are used to detect modifications and malicious code in files on disk);
- the second is based on centralized monitoring (there is embedded support of logging into the central server by ciphering and authentication of connections);
- the third one provides protection against hacking (databases, configuration and log files, e-mail reports, which can contain hidden operations, etc.) [25].

The system supports centralized and distributed control, as well as adaptation and scaling, which are possible according to the number of hosts (if this software is activated on the server), at which notification and detection of UAS activity are performed. Surveillance of this activity in Samhain is carried out only at the system level, and response to cyber-attack is performed in real-time.

VI. CONCLUSION

The experimental results have confirmed the hypothesis that the analysis of software for intrusion detection by basic criteria allows developers and users to select open-source software for IS protection.

Herewith, it should be mentioned that the use of modern means of protection against cyber-attacks does not guarantee absolute security, since, at present, there is an increase in attacks targeting corporate systems, public, confidential, and governmental data resources; cyber-attacks are being continuously modified, improved and become more regular; detection of cyberattacks by classic protection means is not always efficient; advanced attacks on IS are more frequent. This is also related to intensive development of hard- and software as well as globalization of data networks and their daily use in all spheres of social activities.

Therefore, further studies can be devoted to the analysis of integrated engineering solutions for systems of intrusion detection and prevention.

REFERENCES

[1] W. Zhao, and G. White, A collaborative information sharing framework for community cybersecurity, in IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, (2012) 457-462. https://doi.org/10.1109/THS.2012.6459892.

[2] I. E. Lyubushkina, E. M. Zverev, and A. V. Sharamok, Implementation of information security devices in equilibrium codes, Journal of Theoretical and Applied Information Technology, 98(23)(2020) 3909-3920.

[3] A. Bondarenko, and K. Zaytsev, Studying systems of open source messaging, Journal of Theoretical and Applied Information Technology, 97(19)(2019) 5115-5125.

[4] A. Kolychev, and K. Zaytsev, Studying open banking platforms with open source code, Journal of Theoretical and Applied Information Technology, 97(11)(2019) 3038-3052.

[5] M. S. Hoque, A. Mukit, and A. N. Bikas, An implementation of an intrusion detection system using genetic algorithm, International Journal of Network Security & Its Applications, 4(2)(2012) 109-120.

[6] H. J. Liao, C. H. R. Lin, Y. C. Lin, and K. Y. Tung, Intrusion detection system: A comprehensive review, Journal of Network and Computer Applications, 36(1)(2013) 16-24.

[7] A. P. Singh, and M. D. Singh, Analysis of the host-based and network-based intrusion detection system, International Journal of Computer Network and Information Security, 6(8)(2014) 41-47.

[8] W. Park, and S. Ahn, Performance comparison and detection analysis in snort and suricata environment, Wireless Personal Communications, 94(2)(2017) 241–252.

[9] Y. Lin, Y. Zhang, Y. – J. Ou, The Design, and Implementation of Host-Based Intrusion Detection System, in 2020 Third International Symposium on Intelligent Information Technology and Security Informatics, Jian, China, (2010) 595-598. https://doi.org/10.1109/IITSI.2010.127

[10] N. M. Jacob, and M. Y. Wanjala, A Review of Intrusion Detection Systems, Global Journal of Computer Science and Information Technology Research, 5(4)(2017) 1-5.

[11] H. Jin, G. Xiang, D. Zou, F. Zhao, M. Li, and C. Yu, A guest-transparent file integrity monitoring method in a virtualization environment, Computers & Mathematics with Applications, 60(2)(2010) 256–266.

[12] C. A. Catania, and C. G. Garino, Automatic network intrusion detection: Current techniques and open issues, Computers & Electrical Engineering, 38(5)(2012) 1062-1072.

[13] G. Jakobson, Mission-centricity in cybersecurity: architecting cyber-attack resilient missions, in 2013 5th International Conference on Cyber Conflict (CYCON), Tallinn, Estonia, (2013) 1-18.

[14] N. Ben-Asher, and C. Gonzalez, Effects of cybersecurity knowledge on attack detection, Computers in Human Behavior, 48(2015) 51–61.

[15] R. Patel, A. Thakkar, and A. Ganatra, A Survey and Comparative Analysis of Data Mining Techniques for Network Intrusion Detection Systems, International Journal of Soft Computing and Engineering, 2(1)(2012) 265-260.

[16] O. Lawal, Analysis and Evaluation of Network-Based Intrusion Detection and Prevention System in an Enterprise Network Using Snort Freeware, African Journal of Computing & ICT, 6(2)(2013) 169-184.

[17] R. Mitchell, and R. Chen, A survey of intrusion detection in wireless network applications, Computer Communications, 42(2014) 1-23.

[18] E. H. Spafford, and D. Zamboni, Intrusion detection using autonomous agents, Computer Networks, 34(4)(2000) 547–570.

[19] J. Sen, An Agent-Based Intrusion Detection System for Local Area Networks, International Journal of Communication Networks and Information Security, 2(2)(2010) 128-140.

[20] G. Vigna, and R. A. Kemmerer, NetSTAT: A Network-based Intrusion Detection Approach, in Proceedings 14th Annual Computer Security Applications Conference (Cat. No.98EX217),

Phoenix, AZ, USA, (1998) 25-34. https://doi.org/10.1109/CSAC.1998.738566.

[21] C. Wang, Y. Cai, Q. Zhou, and H. Wang, ASAX: Automatic security assertion extraction for detecting Hardware Trojans, in 2018 23rd Asia and South Pacific Design Automation Conference (ASP-DAC), Jeju, (2018), 84-89. https://doi.org/10.1109/ASPDAC.2018.8297287

[22] A. Hay, D. Cid, and R. Bray, OSSEC Host-Based Intrusion Detection Guide. Elsevier Inc., 2008, 307 p. Available: http://index-of.co.uk/Hacking-Coleccion/OSSEC%20Host-Based%20Intrusion%20Detection%20Guide.pdf.

[23] R. K. Jain, and P. Trivedi, OSSEC Based Authentication Process with Minimum Encryption and Decryption Time for Virtual Private Network, in 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN), Tehri, (2016) 442-445. https://doi.org/10.1109/CICN.2016.92.

[24] K. Nam, and K. Kim, A Study on SDN security enhancement using open source IDS/IPS Suricata, in 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, (2018) 1124-1126. https://doi.org/10.1109/ICTC.2018.8539455

[25] M. Nel, SAMHAIN: Host Based Intrusion Detection via File Integrity Monitoring. SANS Institute, (2014) 27 Available: https://www.sans.org/reading-room/whitepapers/detection/samhain-host-based-intrusion-detection-file-integrity-monitoring-34567

[26] Mohammad Dawood Momand, Dr Vikas Thada, Mr. Utpal Shrivastava, Intrusion Detection System in IoT Network, SSRG International Journal of Computer Science and Engineering 7(4) (2020) 11-15.