STM JOURNALS

Journal of
Computer Technology & Applications

ISSN: 2229-6964 (Online)
ISSN: 2347-7229 (Print)
Volume 15, Issue 1, 2024
January–April
DOI (Journal): 10.37591/JoCTA

http://computerjournals.stmjournals.in/index.php/JoCTA/index

Review JoCTA

IT Security and Intrusion Detection Systems: An Introduction

Seyfali Mahini*

Abstract

This article deals with the current status of IT security in an industrialized country and one of the many approaches. The emphasis is on what are known as intrusion detection systems. These enable users to detect suspicious behavior and attacks in daily IT operations by analyzing data, resources, and network flows. Based on previous research, the different variants, available detection types, and their working methods are briefly explained and presented. The primary emphasis should be on understanding the functioning of the systems, their applications, and the constraints that govern them. The aim of the work is to select a suitable intrusion detection system for a hypothetical university such as SafeUni, its data center and the computer labs. This will be done after the mediation of the basics, an abbreviated requirements analysis is presented and the selected intrusion detection system, which best meets the requirements, is presented. The final stage involves summarizing the discovered information.

Keywords: IT security, intrusion detection system, host-based, network-based, hybrid systems, signature-based, anomaly-based

INTRODUCTION

This article offers a brief introduction to the topic of intrusion detection systems. In the last subsection, the further structure of the scientific work is described.

Current Situation

The current situation of IT security is taking on dramatic forms worldwide. Attackers are becoming more and more inventive and are coming up with new attack techniques and tools almost every minute [1]. For this reason, IT security is increasingly becoming the focus of government, business, and the public. The primary goal is to protect the information, data, and services of all participants and to protect them from manipulation. On the other hand, as can be seen in Figure 1, there has been a sharp increase in new malicious programs or malware over the past few years.

However, this list does not distinguish between Trojans, worms, viruses, multi-platform scripts, etc. In 2019 and 2020, an average of 320,000 new malicious programs were registered per day [1]. However, this number has to be corrected upwards, since it is not always possible to correctly classify the software. For example, “potentially unwanted applications” (PUA) cannot always be clearly defined as malware [1]. To counter the trend of recent years, security experts must constantly improve their defense and analysis measures and adapt them to the multitude of threats. Intrusion detection systems can be used precisely for this purpose. Once installed correctly and configured, it is a powerful tool for detecting unwanted activity and access.

***Author for Correspondence**
Seyfali Mahini
E-mail: my1341post@yahoo.com

Lecturer, Faculty of Computer Engineering, Islamic Azad University, Khoy Branch, Khoy, Iran

Received Date: December 22, 2023
Accepted Date: February 21, 2024
Published Date: April 05, 2024

Citation: Seyfali Mahini. IT Security and Intrusion Detection Systems: An Introduction. Journal of Computer Technology & Applications. 2024; 15(1): 10–17p.

Motivations

The motivation of this scientific work is to develop a comprehensive basic understanding of intrusion detection systems, their working methods, and protection potential. This should answer the questions of what different types there are on the market, how they work exactly, for what purposes the individual systems can be used and where their limits lie. This knowledge base forms the basis for providing SafeUni University with another tool to protect its IT infrastructure. Until now, various tools such as firewalls and anti-virus software have been used [expert interview]. As a result, network traffic from outside and a large part of the IT devices in the company's own network are already secured. After this work, the reader should be able to understand the decision-making process of the selected intrusion detection system based on the requirements analysis.

Structure of the Work

The next section of the scientific work deals with the intrusion detection systems and their various variations. The various placement options and how they work are worked out in the individual subsection. The third section is dedicated to the types of detection and analysis. Each subsection represents a separate approach to configuration and threat detection. The complete topic is then summarized in the last main section and a final conclusion is drawn.

Intrusion Detection

As business and society shift more and more of their day-to-day affairs to complex IT systems, they inevitably become dependent on them. It has become increasingly clear over the past few decades that IT security cannot only be achieved through a reactive concept, but that a preventive approach is required. This means recognizing dangers before they pose a risk to your own systems.

Basic Knowledge

For this reason, and to be able to react to risks and security breaches, research into intrusion detection has been pursued since the mid-1980s [2]. The result of these are the intrusion detection systems (IDS) commonly used today, which are in daily use in many places. These systems differ slightly in their internal structure, but the main components defined in Table 1 can be found in almost every IDS.

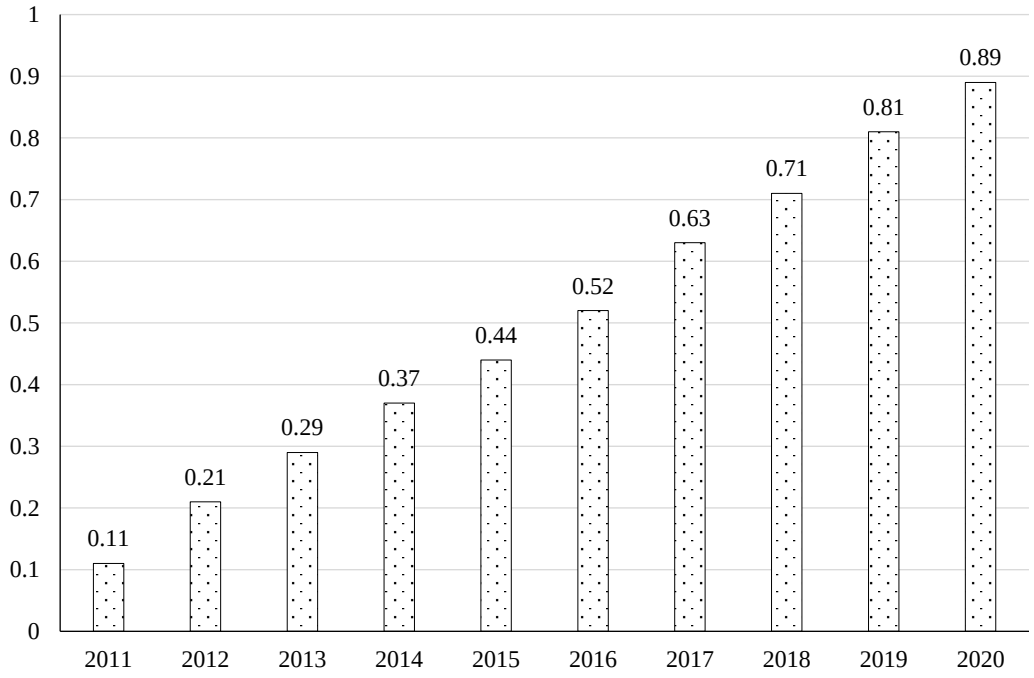

Figure 1. Development of registered malware from 2011 to 2020.

Table 1. Definition of the modules of an intrusion detection system (IDS).

Designation	Description
Sensor	Smallest unit that has, e.g., the task that monitors CPU usage
Agent	An agent is installed on an IT system and coordinates the individual sensors; some of the values are pre-processed here
Analysis unit	This module is responsible for evaluating the collected data, the exact location may vary. Partially integrated in the agent, own module or in the server
Server	This module collects and manages all information centrally. In some cases, all information is evaluated here, and the decision is made as to what results from it

An IDS pursues the task of documenting any unusual behavior and triggering an alarm if necessary. These normally work completely autonomously and only require a few active interventions by the administrators. The focus is on detecting attacks as early as possible in order to minimize the damage caused by the incidents. At the same time, they collect conspicuous behavior patterns in normal operation in order to be able to draw attention to new possible attack methods [3]. The goal when evaluating all of the data is to achieve a high detection rate while getting as few false alarms as possible [4]. The exact definition of an intrusion or an incident, for a host or the network, violates the security guidelines and puts the IT system in an unacceptable state [5]. The following list provides the various system states that an IDS can achieve after the analysis unit has processed the information:

- *True positive:* A change was correctly identified as a risk.
- *True negative:* A change was correctly identified as harmless.
- *False positive:* A change was incorrectly identified as a risk.
- *False negative:* A change was incorrectly identified as harmless.

When optimizing the analysis unit, two classification results pose a challenge. (1) False positive, that is, a safe condition that has been recognized as a risk and (2) false negative, that is, a risk that has not been recognized as such [3]. The prerequisite for successful automatic detection is the quality of the data. A large amount of information is only helpful if it can also be evaluated in good time. It therefore makes perfect sense to only periodically monitor a specific part of an IT system and not to have to handle the entire volume of data. In most cases, the administrators have to set what is observed and how in the configuration files [3]. An IDS always contains the following components: One or more sensors that forward the events to their agents. An analysis unit and a module for reporting, for example, by a server. This can be console output, e-mails or SMS that are sent or the direct report to an intrusion prevention system (IPS) [5].

Depending on the place of use and the type of installation, a distinction is made between the following options, as can be seen in the following list [5].

- *Local installation:* Used to monitor a single IT system. Sensors, agent and server are located on the same IT system.
- *Agent installation:* Used to monitor multiple IT systems. Sensors and agents work with analysis units on the IT system and forward alarm messages to a central installation.
- *Server installation:* extension of the agent installation. Data is forwarded even without an alarm message. The analysis unit sits on an extra server so the information can be processed cumulatively.

In the following subsections, the individual possible uses of the IDS are explained in more detail.

Host Based

A host-based IDS (HIDS), for example, is a software that contains both agent and sensor. It is installed on the IT system to be monitored, such as a server or workstation, and has direct access to the resources. For example, the complete communication stream can be checked before it is presented to the operating system. This means that encrypted communication from the network can still be checked, which could escape a network-based intrusion detection system. Outgoing packets for the network can

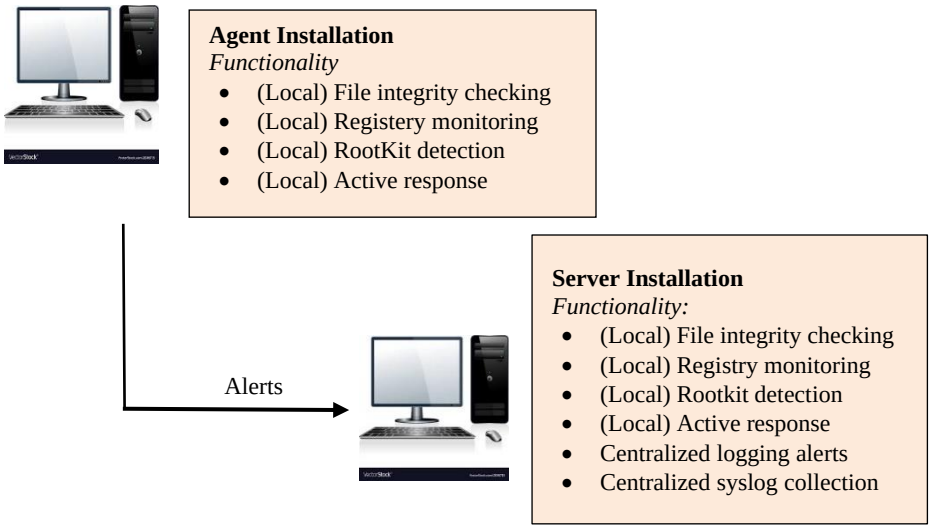

Figure 2. Example of a host-based agent installation [6].

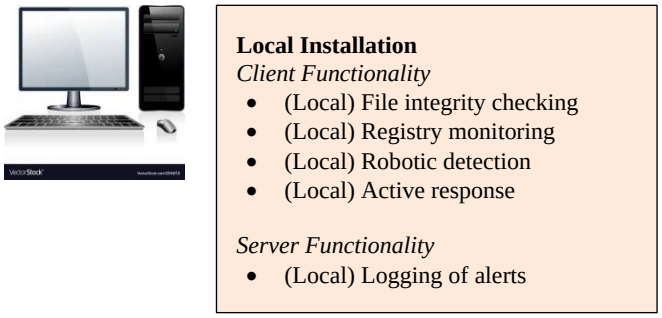

Figure 3. Example of a host-based local installation [6].

also be checked before their own encryption. Since the sensor and agent are installed directly on the host, it has access to important monitoring functions. For example, it has via system-level checks, can check file integrity, monitor changes in the registry, analyze local logs and offer rootkit detection. In addition, some HIDS have an active response to directly prevent greater damage [6]. An example with an agent installation can be seen in Figure 2.

An agent is installed on the IT system to be monitored and the desired functionality is configured. If impermissible states are detected in the individual sensors, an alarm message is sent to the server. This infrastructure allows them to continue to scale until the server has reached its maximum number of clients to be monitored and can no longer process them. Figure 3 is provided to illustrate a local installation. Here the complete monitoring of the IT system is located on a single host.

File Integrity Check

Using a hash function, every file on an IT system forms a unique fingerprint. This depends on the content, the file size and the respective file name and changes with every type of manipulation. If these fingerprints are checked periodically, a change is immediately noticeable and can be checked more closely [6]. The basis for this measure is that the system was in a permissible state at the time the IDS was commissioned.

Registry Monitoring

The system registry is a central directory on a Windows operating system. All hardware and software settings, operating system configurations, as well as users and group policies are managed in a concentrated manner here. Changes to it, whether by users or administrators, are saved by keys. A HIDS

can watch for changes in these important keys by periodically checking. This immediately detects malicious intentions by users or programs that want to install a new program, for example [6]. *Assumption:* The system was in a valid state at the time of installation.

Rootkit Detection

Rootkits have existed since the 1990s. They are to be seen as a back door through which attackers can move as an administrator (root) [7]. Well-hidden in the system, it interacts with the system. The rootkit can hide ports, files, directories, services and registry keys from the user. The most common type of rootkit, the application-level rootkit, replaces original application binaries with their own modified versions. At this point, the detection type works similar to the file integrity check. In the case of rootkits at the kernel level or virtualized rootkits between hardware and operating system that manipulate system calls, detection becomes more difficult [6].

Active Response

As a direct response to threats, HIDS can intervene in the ongoing operation of the IT system by executing predefined commands. For example, ports can be blocked, the execution of a questionable program blocked, or an alarm issued. IPSs that are addressed directly and that can initiate more extensive countermeasures also benefit from this functionality. As great as the benefits of one of these active response units are, they also offer great risk potential. False-positive system states can, for example, disrupt operations or bring them to a standstill. Often triggered by poorly defined rules or inaccurate observation of anomalies [6].

Network Based

The network-based intrusion detection systems (NIDS) work as separate network participants or expand, for example, a firewall (FW). Their task is to analyze the data traffic in the network segment and to raise an alarm if there is anything unusual. To distinguish between the two systems: A firewall protects against attacks from and to the outside, a NIDS protects and analyzes the data traffic in its own network. A combination is therefore highly recommended and can be seen in Figure 4.

This configuration inspects all packets moving over the network [4]. In order to get all packets in a modern network, the switch must have a mirror port function. This means that all traffic from the switch is also forwarded to the NIDS. This requirement did not exist in earlier setups with network hubs. A major disadvantage of the NIDS is the required bandwidth and the computationally intensive evaluation of the packets [4].

Hybrid Systems

Hybrid IDS have the advantage that the HIDS and the NIDS complement each other. In the best case, all agents deliver the information they have obtained to a central server. In this way, these findings can

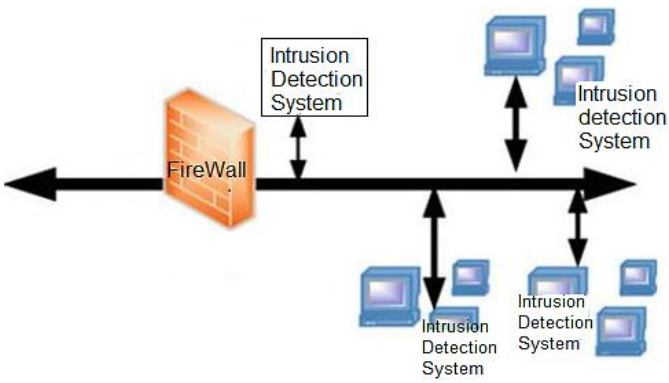

Figure 4. Sample structure of a hybrid intrusion detection system (IDS) [4].

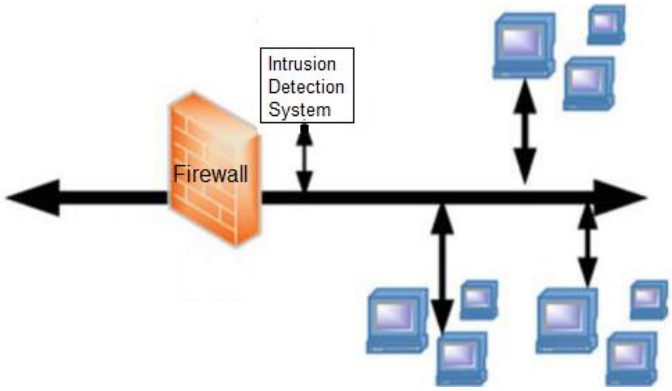

Figure 5. Combination of network-based intrusion detection system (NIDS) and firewall in a network [4].

be processed cumulatively and provide more precise statements on the current risk situation. An example setup is shown in Figure 5. Here the entire network is protected from the outside by a firewall, the internal network traffic is monitored by NIDS and important IT systems also have HIDS. In the optimal case, all findings are analyzed at a central point in order to be able to make the most accurate predictions.

DETECTION METHODS

Basically, all IDS, whether HIDS or NIDS, work with three different detection methods. Each of these requires data for analysis and comes with its own strengths and weaknesses. A combination of different approaches is definitely recommended or is common.

Rules-Based

Probably the simplest form of filtering is the rule-based approach. It is fed by a set of hard, pre-configured rules and restrictions and blocks or allows exactly this type of event. This detection method is only as good as its configuration and cannot detect anything else [4].

Signature-Based

Signature-based IDSs use known signatures or attack patterns to detect malicious behavior. They are suitable for recognizing already known attacks with little effort. If so-called zero-day exploits or newer methods are used, the signature-based IDS are not effective in detecting a threat. It is important that the signatures are updated regularly so that the protective function is maintained. There are open-source approaches as well as commercial providers [4]. In general, this method provides robust and sharp results, on the basis of which action can be taken [3].

Heuristic Methods

Heuristic methods, also known as anomaly-based detection, are the means of choice when it comes to detecting previously unknown attack patterns. This detection method defines an explicit value for normal behavior of the IT systems. Depending on the threshold set, an anomaly, that is, a deviation from normal behavior, triggers an alarm message. The problem are that not every unnatural behavior has to be an alarm state. Another disadvantage is the detection rates of such methods for known attacks. These are inferior to the signature-based detection methods and do not produce such reliable results [3, 4].

INTRUSION DETECTION SYSTEM FOR THE SAFEUNI

The aim of this scientific work is the well-founded selection of a suitable IDS, according to the requirements of the computer center (CC) of the intended university.

In the first step, a requirements analysis was carried out. An employee of the CC was available for an expert interview. During the conversation, the existing and future IT infrastructure was discussed,

Table 2. Primary requirements of the data center for an intrusion detection system (IDS).

Designation	Description
A1	The system that does not entail any additional (license) costs
A2	The focus of the desired system is on the individual host systems, e.g., in the laboratories
A3	The agents or sensors must not exclude any operating system (Windows, Linux, MacOS)
A4	The system should not noticeably restrict the use of the hosts or the user
A5	The system must be expandable with specially written modules in order to be able to react to every conceivable case

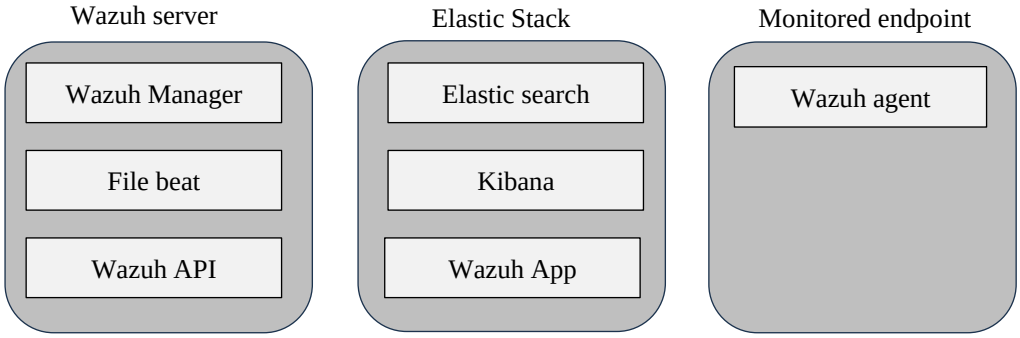

Figure 6. Server installation of Wazuh.

previous attacks and incidents were discussed, and wishes and suggestions for the new system were also expressed. Based on this discussion, requirements were derived and weighted. The most important findings from this are listed in Table 2. These are the primary requirements that must be met in order to qualify for a software solution.

Based on the primary requirement A2, a HIDS was sought, while the NIDS were not considered in the selection process. The requirements A1 and A5 led the research to various open-source projects, with broad community support. Requirement A3 could be clarified through research and for A4 the system requirements, the sensors and agents, were considered. The evaluation, through a table with weighting of the properties of the researched HIDS, revealed a promising candidate – the current version of Wazuh [8]. This is an actively maintained fork of the well-known HIDS OSSEC. Wazuh provides a security solution capable of monitoring your infrastructure, detecting threats, intrusion attempts, system anomalies, poorly configured applications, and unauthorized user actions. It also provides a framework for incident response and regulatory compliance. The distributed installation, also known as the server installation from the previous chapters, has three main components. These can be seen in Figure 6. The three pillars are discussed in more detail below.

The Wazuh agent, the right column in Figure 6, provides the sensors for various IT systems and tasks. This includes file integrity checks, collection of log and registry data, listing of running processes and installed programs, monitoring of open ports and network configuration, and other functions. Administration and configuration run via the Wazuh server. The Elastic Stack, in the middle column in Figure 6, offers the possibility to clearly visualize the collected data. There are ready-made dashboards for the web interface, which can be modified as desired. For this purpose, Kibana [8] was integrated into the Elastic Stack.

The last column, on the far left in Figure 6, represents the Wazuh server. Its task is to analyze the data received from the agents and to evaluate the results using rules and other methods. In daily operation, a single Wazuh server can serve hundreds of agents and is scalable when installed in cluster mode. Another great advantage of the selected HIDS is that the agents can be configured and updated remotely. The server can also send commands to the agent in order to protect itself against a detected attack.

CONCLUSION

The result of this work is the realization that there are some very potent approaches in the open-source segment of the IDS. Differences are often the range of functions, the performance and the purpose of the applications. Some systems build on each other or use the same code modules. With regard to this work, it can be considered a success that all primary requirements for the IDS were met, and a corresponding software solution was found. In addition, Wazuh offers additional functionality, such as configuring the agents over the network, which were not part of the primary requirements.

REFERENCES

1. Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. J Computer Syst Sci. 2014; 80 (5): 973–993.
2. Brooks DJ, Coole MP. Intrusion detection systems. In: Shapiro LR, Maras M-H, editors. Encyclopedia of Security and Emergency Management. Cham, Switzerland: Springer International Publishing; 2021. pp. 490–494
3. Khraisat A, Gondal I, Vamplew P, Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity. 2019; 2 (1): 1–22.
4. Kim K, Aminanto ME, Tanuwidjaja HC. Network Intrusion Detection Using Deep Learning: A Feature Learning Approach. New York, NY, USA: Springer; 2018.
5. van Oorschot PC. Computer Security and the Internet. Cham, Switzerland: Springer International Publishing; 2020.
6. Cid D, Hay A, Bray R. OSSEC Host-Based Intrusion Detection Guide. Burlington, MA, USA: Syngress; 2008.
7. Kraft P, Weyert AG. Network Hacking: Professionelle Angriffs-und Verteidigungstechnikengegen Hacker und Datendiebe. Haar, Germany: Franzis Verlag; 2017.
8. Shukla P, Kumar S. Learning Elastic Stack 7.0: Distributed Search, Analytics, and Visualization Using Elasticsearch, Logstash, Beats, and Kibana. Birmingham, UK: Packt Publishing Ltd; 2019.

