Celal Bayar University Journal of Science

Comparison of the Host-Based Intrusion Detection Systems and Network-Based Intrusion Detection Systems

Ahmet Efe[1]*, İrem Nur Abacı[2]

[1]PhD, CISA, CRISC, PMP, International Federation of Red Cross and Red Crescent Societies, Internal Auditing Department, Ankara, Turkey
[2]Gazi University, Department of Computer Sciences, Ankara, Turkey
* icsiacag@gmail.com
*Orcid: 0000-0002-2691-7517

Received: 27 November 2020
Accepted: 24 January 2022
DOI: 10.18466/cbayarfbe.832533

Abstract

Advanced Persistent Threat (APT) has recently emerged as sophisticated and tailor-made attacks. APTs pose threats mainly targeting military, defense, security infrastructure, high profile companies, and government units. Intrusion detection mechanisms are crucial for adequate protection, especially as a countermeasure for APT attacks done by hacktivists, cyber warriors, and cyber terrorists over management information systems (MIS) of government institutions and e-government applications. In this study, Intrusion detection and prevention systems have been studied in detail after being referred to the tasks and abilities of the intrusion detection systems that are at the core of the computer security technology presented today to meet the increasing need for information and network security. This paper aims to specify the differences between Host Based Intrusion Detection Systems (HIDS) and Network-Based Intrusion Detection Systems (NIDS) and compares the tools using HIDS and NIDS. It is asserted that to better assurance for APT attacks, there should be a Hybrid IDS approach covering both networks and hosts using both signature and behavioral detection mechanisms based on deep learning algorithms.

Keywords: Intrusion detection systems, Host-based intrusion detection systems (HIDS), Network-based Intrusion detection systems (NIDS), Hybrid IDS, MIS security

1. Introduction

One of the main issues of trust in E-government implementation is security. The information age makes information to be accessed all over the world without any constraints due to the usage of technological advancement that provides solutions for efficiency, confidentiality, and availability concerns. Citizens prefer to use traditional ways rather than an unsecured website [1]. So information services located on servers become widespread, and data stored on these services become vulnerable to exposure and cyber-attacks. Mainly cloud services provide omnipresent opportunities for information processing and fast access, and it also makes information more vulnerable a target for hacktivists, cyber warriors, and cyber terrorists. Cyber-attacks have existed, evolved, and become more sophisticated than ever in recent times as Advanced Persistent Threats (APTs) come into view.

Along with the widespread use of the internet, threats to information systems have also increased dramatically and widened in types of attacks. Along with the rapid increase in the number and types of security threats, security technologies are also undergoing rapid development. Security mechanisms such as authentication and access control were first developed to ensure the security of computers, prevent unauthorized access to systems, and capture or modify information. Such mechanisms constitute the first step of safety. Firewalls, vulnerability scanners, and intrusion detection systems form the second stage of security mechanisms. None of these security technologies alone is fully adequate because each one is focused on different security points. For a secure system, these structures must be used together to support each other. The purpose of intrusion detection is to classify all intrusion attempts correctly and notice activities that should not be tagged as an intrusion. In this context, an intrusion is a resource accessibility violation. Systems that detect these actions are named

Intrusion Detection Systems-IDS. IDS use system network or data to find attacks.

IDS provides three essential security functions: monitoring, detecting, and responding to unauthorized activities. IDS are generally classified as follows [2]:

1. Host-Based (HIDS): Host-based intrusion detection systems run on individual hosts/devices on the network.
2. Network-Based (NIDS): Network-based intrusion detection systems monitor traffic between all devices on the network.

In general, the effectiveness of the intrusion detection system depends on its "Configurability" (Ability to define and add new specifications attack), robustness (fault tolerance), and the small number of false positives (false alarms) and false negatives (undetected attacks) it generates [3]. The remainder of the paper is organized as follows: Introduction to intrusion detection systems; advantages and disadvantages of both network-based IDS and Host-based IDS; expectations from sound intrusion detection systems; intrusion detection tools; and conclusions are drawn before future work discussed.

2. The E-Government Security Risks to Be Mitigated by IDS Systems

According to a study, the development of e-government faces fatal security problems due to the complexity and vulnerability of networks [4]:

2.1 Information Intercepting

If interceptors cannot be detected in a system, information confidentiality will not be adequately managed.

2.2 Information Tampering

If information tampering cannot be detected in a system, information integrity and availability will not be appropriately managed.

2.3 Services Denying

It is the complete invalidation of the network system or the server's system in some period.

2.4 System Resources Stealing

In the network system environment, stealing the system resources is very common.

2.5 Information Faking

The primary forms include pretending users get illegal certifications, forging emails, etc. The risks mentioned above related to e-government applications and e-business systems can be mitigated by using IDS systems properly.

3. Intrusion Detection Systems-IDS

Intrusion means any set of actions that dare to risk a source's integrity, confidentiality, or availability. Such computer system violations can cause problems: data integrity, access denied for online resources, the leak of confidential data, and taking benefit of private resources. Denning implemented an intrusion Detection System (IDS) in 1987. Since then, IDS has become a hot analysis topic essential for network security. IDS protects external users and inner attackers, wherein visitors do not pass beyond the firewall at all. Intrusion Detection Systems are divided into identification methods and attack detection.

Intrusion Detection Systems are based on their established environment; Network Intrusion Detection Systems and Host-based Intrusion Detection Systems. Intrusion Detection Systems are divided into signature-based Intrusion Detection Systems and anomaly-based Intrusion Detection Systems according to intrusion detection methods. Signature-based Intrusion Detection Systems use attack signatures in an attack signature database to detect attacks. Anomaly-based Intrusion Detection Systems perform intrusion detection based on the anomalies in the network traffic without using attack signatures. Signature Based Intrusion Detection Systems can only detect attacks on the attack database. They have no chance of seeing new episodes. Since anomaly-based Intrusion Detection Systems do not use any attack signatures, these systems are likely to produce false-positive results. Anomaly Based Intrusion Detection Systems are also able to detect new attacks. Intrusion detection systems are systems designed to detect these attacks, which are made up of various packages and data, which can be attacked or caught after computer system attacks against the computer system technology. Intrusion detection systems can be thought of as a kind of alarm system.

It is possible to divide them into categories in many different ways. For example: According to the Internet Security Systems (ISP) model, an intrusion detection system can be primarily active or passive. The latter may be host-based or network-based. When we combine these two systems, intrusion detection systems can be grouped as such:

- active / host-based,
- active / network-based,
- passive / host-based,
- passive / network-based.

Intrusion detection can be classified according to two analysis methods. A system needs to respond in real-time or close to an attack that is detected to be functional (for example, shaping firewall rules against an attack or warning the user from the command console). Passive systems usually record episodes and

then store them for review. There is a need for triggering mechanisms (in other words, to know the wrong and unusual usage of the system and network resources) to detect attacks. These are misuse attacks (signature-based attacks) and anomaly attacks.

Intrusion Detection is becoming re-created as Intrusion Prevention. These systems are being crafted for HIDS and NIDS environments, showing that vendors listen to security needs. These new technologies work by various means, such as intercepting application interface calls to operating systems and classifying the calling activity. If the Intrusion Prevention system thinks that the caller is inappropriate, the access can be denied, allowed, logged, or combined.

3.1 Network-Based IDS

A Network-Based IDS (NIDS) analyzes incoming packets over a network connection and analyzes packets on the data part of the attack. NIDS uses the abnormality detection of signatures to detect attacks. It alarms to report a real-time attack keeps a log of detailed information about the attack after the attack has occurred. Network-based intrusion detection systems display the traffic passing through the network's segment in the form of a data source. This is usually accomplished by bringing the network card into promiscuous mode to capture all traffic passing through it. Traffic to other segments of the network and other types of communication, such as phone lines, can not be captured and displayed. The network-based intrusion detection system mainly deals with packets passing through the network via a sensor. The package arriving at the detector must be checked against the existing signatures to decide what to do with the package. The filter at the start level specifies which packets are accepted and which packages are to be discarded or sent to the attack recognition module. If an attack is detected, the response module triggers the alarm to be generated in response to the attack. Encryption of the traffic between the sensor and the monitor, including sensors and viewers in a separate network, is essential for security. For a knowledgeable and experienced attacker, the traffic (alarms, status logs, other packets, etc.) between the sensor and the viewer is vital for attacking the network. Sensors and viewers can be included in a separate network to protect against DoS (Denial of Service) attacks. The other advantage is that the network on which the attack is detected differs from the network we are on.
Network-based intrusion detection relies on acquired knowledge [6]. Symantec reported that IDS could generate 10-90% of false alarms depending on the level of tuning and customization [7]. Julich and Dacier [8] have pointed out that IDS could generate up to 99% false alarms.

3.2 Host-Based IDS

Host-based intrusion detection was a commonly used method in the early 1980s. Audit logs were held against potentially dangerous network activities. Today, this system is used; but "audit logs" are more sophisticated, automated, and real-time detection and response made easier. Software is used to view logs in host-based systems. The system, event, and security records on Windows NT systems, Syslog, and custom OS registry files are available on UNIX systems. Any changes to these files are to be compared to the existing security policy, and the response will be promptly answered. The host-based IDS displays real-time logs and responds in the same way. Some host-based IDS can also listen to port events and block access to specific private ports, thereby providing network security. The task of host-based intrusion detection systems; Listening to the traffic of the server on which the server is installed, recording files and transactions based on the attack/signature database on the server and customized for that server, and responding by detecting attacks. Host-Based Intrusion Detection Systems (HIDS) work by examining the log files of the server traffics based on the database on the server and notify a report to the relevant system administrator when an unexpected attack is detected. The essential rule in these systems is system compatibility. The compatibility of operating systems can be non-contingent.

Host-based intrusion detection systems are installed on various special servers and detect or prevent attacks on that server. It is the task of taking the configuration files of the systems they are in, tracking the files that the system records are kept in, examining the changes that may occur in the system's integrity, and preventing malicious use. They have difficulties complying with the systems they have built fully. The nature of the operating systems is incompatible with each other. This leads to the requirement that intrusion detection systems are explicitly written for that operating system and structured to the weaknesses. They are available for custom server software.

4. Literature Review

Anderson first described the concept of the intrusion detection system in 1980, and in 1987 by Denning's publication, the basic intrusion detection system was defined. The amount of data being produced by such Intrusion Detection Systems (IDS) exceeds by far the human capability of information processing [9]. Various researchers have given the following definitions on matter intrusion detection systems and technology in recent years.
According to Yang and others [10], IDS is a system that detects and identifies intrusion behavior or intrusion enterprises by monitoring and analyzing Ag

packets or system audit records in a computer system and then giving real-time intrusion warnings to system administrators.

According to Xuetao and others [11], intrusion detection technology is a crucial research area in the information system, which is open to attack and is an essential research direction for information technologies that prevent malfunctions from being exploited by malicious codes or codes.

According to Pikoulas and others [12], the intrusion detection system is a system that identifies threats aimed at any organization and then guarantees that the system is protected.

Jemini and others [13] have compared a network with an intrusion detection system to a house with installed burglar alarm systems. They both used different methods to detect an attacker from the inside. In addition, everyone has been alerted that the system and the attacker are alerting them.

From the above definitions, the definition of the intrusion detection system, in general, can be given as follows: It is a system aiming at detecting attackers who are infiltrating or leaking outside the system with various purposes such as accessing the system without permission, unauthorized use of the system resources, accessing and changing the personal information of the users, running or stopping the operation of the system, and users who misuse the limited system resources.

Intrusion detection systems can be divided into three main categories and subcategories. Network-based intrusion detection systems detect web-based attacks based on an intrusion detection system and host-based intrusion detection systems that detect attacks against a single computer system. Traditionally, intrusion detection systems detect misuse attacks and systems that see anomaly attacks. According to the attack detection technique, some studies assumed that they are in systems that detect identification/hybrid attacks, a mixture of misuse and abnormality models, as an additional category [14,15]. Also, detection of abnormality attacks can be decomposed by statistical abnormality test, artificial neural networks, full based on the detection of abnormality, data mining based on the detection of anomalies, immune-based abnormalities detection, and so on [10,16].

Intrusion detection systems are central and distributed according to their architectures [14,17]. Data analysis in centralized intrusion detection systems is done on a server independently of the number of servers monitored. This process can be done on servers in the intrusion detection systems prepared with distributed architecture. Though centralized architecture and intrusion detection systems have the advantage of having direct access to the database, there is a severe drawback, such as the occurrence of bottlenecks. DDIS, AAFID, and NIDIA can be given to intrusion detection systems prepared with distributed architecture. Intelligent agents are usually used in structures used instead of the new generation distributed architecture. Intrusion detection systems can be classified as real-time or offline in terms of operational logic.

A STUDY USES XML-based SOAP, WSDL, and UDDI to utilize web services that allow machine-to-machine interoperability. M. Silva and others presented a multi-agent remote access intrusion detection system [17] that provides services for users who do not have a local intrusion detection system in their work. Multi-agent architecture and model-based architecture web services were used in the model they used. Due to the multi-agent structure, system flexibility is provided by agents sharing information in the system. Model-based architecture adds portability, interoperability, and reusability to the system. The design presented in this study consists of 6 layers, including monitoring, analysis, response, update, management, storage. The proposed system provides intrusion detection system services over the internet. Although users can easily access it, there is a disadvantage in its very intensive communication.

Data collection techniques in intrusion detection systems are implemented through sensors. These sensors are classified as internal and external sensors. Internal sensors embedded in the program being watched or working as part of them and those separate from the program are also referred to as external sensors. Advantages of external sensors; They can be easily added to the server quickly and easily separated from the server. The ability of an attacker to disable or change the sensor as easy to modify and creating delays is the disadvantage of external sensors. The advantages of internal sensors can be listed as minimal latency, ease of change, and difficulty in developing the server's weaknesses. However, it is listed as a low overhead to the server's performance, the necessity of developing the program to be monitored in the program's language, updating and developing the wrong implementation, and serious problems. Examples of external sensors are agents that monitor each server in distributed systems separately and report them in a hierarchical structure they find. Internal sensors developed for OpenBSD systems for internal sensors can be provided that do not require the additional load to detect different attacks in real-time [15]. Intrusion detection systems' quality should be evaluated according to their effectiveness, adaptability, and extensibility scales [15].
While intrusion detection systems detect attacks, they do not determine that they have failed successfully. Instead, this decision is left to the analyst and system

administrators. In such a case, the system administrator reviews the collected audit information, performs vulnerability scans, and checks the system for updates. Although these operations can be performed on small-scale networks, they are not practical in distributed networks having a large amount of control information.

Researchers have generally ignored the human factor by focusing on the machine component in the intrusion detection system. This shortcoming puts the advocating side in a disadvantageous position. Because the values of avoidance and assertion validation methods are not fully understood [16].

5. Verified Current Zero-Day Exploits of IDS Systems

The zero-Day vulnerability occurs when computer vulnerability is publicly announced. Once the Zero-Day Vulnerability occurs, all computers and computer users using that software are at risk. If the software's support team does not act fast enough to close the gap, hackers can turn this vulnerability into exploits and quickly share them among themselves. Of course, a competent team can perform a simple computer user or internet hackers. As a result, more hackers can easily manage to exploit this vulnerability.

Zero-Day Exploit transforms the vulnerabilities caused by the Zero Day Vulnerability into software or scripts by experienced internet hackers. When such vulnerabilities are turned into Zero-Day Exploit, all professional or inexperienced hackers can easily exploit the vulnerability and damage systems.

The preparation of Zero-Day Exploits is sometimes a complicated process, and sometimes it can be straightforward. Creating Zero-Day Exploits for operating systems such as Windows XP that have entirely lost support and have not received updates will be much easier. Microsoft has announced that no security updates will be offered for this operating system. All vulnerabilities for Windows XP will turn into Zero-Day Exploit from now on.

Zero-Day Attack attacks can be a kind of blessing for internet hackers who act early. A zero-day attack is the emergence of software vulnerability and hackers launching attacks using this vulnerability directly or as an exploit. Because although others have revealed these vulnerabilities, the first act of hackers will benefit from this vulnerability and will continue to use the exposure until closing the gap. Some examples of IDS and systems are declared as verified zero-day exploits in the table below. The hyperlinks can provide detailed information for each exploit.

Table 1. Some Examples for Verified Exploits Declared in the Exploit Data Base on the IDS

Date	Title	Type	Platform	Author
2009-09-21	Snort unified 1 IDS Logging - Alert Evasion & Logfile Corruption/Alert Falsify	DoS	Multiple	Pablo Rincón Crespo
2009-07-27	Magician Blog 1.0 - 'ids' SQL Injection	WebApps	PHP	Evil-Cod3r
2007-12-26	RunCMS 1.6 - Blind SQL Injection (IDS Evasion)	WebApps	PHP	sh2kerr
2007-10-27	Oracle 10g - 'LT.FINDRICSET' SQL Injection (IDS Evasion)	Local	Multiple	sh2kerr
2005-12-07	Appfluent Database IDS < 2.1.0.103 - Environment Variable Local Overflow	Local	Solaris	c0ntex
2002-05-17	Cisco IDS Device Manager 3.1.1 - Arbitrary File Read Access	Remote	Hardware	Andrew Lopacki
2001-09-05	Cisco Secure IDS 2.0/3.0 / Snort 1.x / ISS RealSecure 5/6 / NFR 5.0 - Encoded IIS Detection Evasion	Remote	Multiple	blackangels
2000-06-07	Computer Associates eTrust Intrusion Detection 1.4.1.13 - Weak Encryption	Local	Windows	Phate.net
1999-08-05	Network Security Wizards Dragon-Fire IDS 1.0 - Command Execution	Remote	Hardware	Stefan Lauda

Source: www.exploit.db

The information given in Table 1 is related to exploits available in the exploit database for the IDS system. The each of the exploits, there is a link demonstrating its information. For example, with the "Snort unified 1 IDS Logging - Alert Evasion & Logfile Corruption/Alert

Falsify" named exploit, the alert type and size are overwritten with the MAC addresses of the raw packet.

So with malformed packets (Eth/IP/TCP/Data with modified MAC addresses), the size and the type (and other information) can be set falsifying alerts for a later parsing process. For example, suppose an attacker builds malformed packets. In that case, so a signal is faked, the size is more extensive than 128M (the unified log limit size by default), snort will continue inserting alerts in the file. Still, when reading that alert, a parser

will try to jump 128M skipping the signals inserted after the falsified one. An attacker can also insert a complete list of falsified signals and malformed packets because the basic package is TCP data. You can fill with falsified UnifiedLog alert structures with binary data. Therefore you would need to adjust the packet headers to set the "size of the alert" (overwritten with the MACs of the packet), making that the parser read the following alert in the offset that the TCP data will overwrite with the list of falsified warnings.

6. Advantages and Disadvantages of NIDS and HIDS

According to the intrusion detection system, the categorization is performed single host-based or multi host-based because of data collection mechanism and activities monitoring. Network-based intrusion detection systems monitor the entire network to determine an attack or an attack condition. There is a distinction between network-based and host-based systems on "how data is collected" but not on "how and where data is processed" [15]. In general, network-based intrusion detection systems are based on signature detection, and host-based intrusion detection systems are based on anomaly detection [14,15]. The HIDS and NIDS approaches have advantages and disadvantages. Pahlevanzadeh and Sansudin also exhibited these advantages and disadvantages that they have stated in their work in Table 2.

Table 2. Comparison of HIDS and NIDS

NIDS	HIDS
The activity area is wide	The activity area is limited. It monitors private system activities.
It is better at detecting an attack from the outside. Notices that HIDS is missing	It is better at detecting intrusions from inside. HIDS notices that NIDS are missing.
The package header and the entire package will be examined.	It does not see package headers.
The reaction is close to real-time.	Reacts after any suspected entry.
Independent from host	Dependent to host
Dependent to bandwidth	Independent from bandwidth
Slows traffic on networks where IDS clients are located	Slow down IDS installed server computers
The payload detects network attacks after they are analyzed.	Detects local attacks before they damage the network.
It is not appropriate for carrying encrypted data and using the keying.	It is appropriate for carrying encrypted data and using the keying.
There is no overload	Overloaded
Have high false-positive value	Have low false positive value

In addition to the information given in Table 1, Bai and Kobayashi [15] point out that it is difficult to change the evidence left by the attacker for network-based intrusion detection systems and host-based intrusion detection systems are connected to the operating systems. However, they will not miss packets such as network-based systems in dense network traffic [18].

The goal of the NIDS is to detect an attack that is actively happening on a network. The emerging trend seems to blend the two approaches in what we now call a hybrid intrusion detection system [19]. The Hybrid IDS combines both signature and anomaly-based models to achieve higher detection rates with lower false positives.

In addition to the host and network-based intrusion detection systems, these systems can be considered a mix of host and network-based systems divided into three different categories [15]. These are PH-NIDS (Per Host Network-Based IDS), LB-NIDS (Load Balanced Network-Based IDS), FW-IDS (Firewall Based IDS). PH-NIDS analyzes network traffic based on the host and only incoming traffic. LB-NIDS uses load balancing and balances bandwidth using other network intrusion detection systems. FW-IDS Network-based intrusion detection system adds functionality to a firewall. There is hardly any packet loss, but there is a slowdown in the network.

7. Expectations from a sound intrusion detection system

The quality of intrusion detection systems is often assessed according to their effectiveness, adaptability, and extensibility characteristics. These parameters can be ordered as follows from a good and quality intrusion detection system other than the primary needs:

- Attack detection rates are at very high levels
- It can operate at high speed and can be used in real-time and applications
- Be able to display all events by following the most effective listening data in large quantities
- In the system where it is running, the processor memory, file, and network operations are at a minimum level of resource utilization
- To Alert the security analyst by instantly alerting them of any attack
- Be able to withstand the attack that may come to it
- Easy to set up and scalable
- No matter how high the density in the network traffic, the network packets are not lost
- It is a structure that does not cause faults and openings in its internal mechanism.
- The system must be very resistant to an attacker's deception.

8. Intrusion Detection Tools

Here we are analyzing some of the best known IDS tools to understand their benefits and advantages in comparison. Snort is a leader in open-source NIDS solutions. Snort uses signature-based intrusion detection and anomaly-based detection methods and can rely on user-created rules or update signatures from the database as emerging threats. Suricata is Snort's direct competitor, and it applies a security and anomaly-based approach based on signature-based detection methodology to detect attacks. Bro IDS uses an anomaly-based intrusion detection method. The language of Bro IDS is specific to network applications that are the NIDS. It is very effective in traffic analysis.

6.1 Snort

Snort is a recently developed network-based intrusion detection system that can perform abuse detection and real-time traffic analysis on IP networks. Snort is an intrusion detection system that works in the abuse detection model—initially presented as a rule-based penetration detection system in the intrusion detection model. Nowadays, it is also used for traffic analysis such as network data collection using plug-in programs detection of abnormalities in protocol headers. Snort consists of a multi-layer structure. It works with all the arrangements to detect specific attacks and output them in the desired format.

Snort, open-source, and free software distributed under the GNU license, was developed by Martin Roesch in 1988. Now, an attack developed by Sourcefire, which Martin Roesch has built, is the most widely used globally. It is capable of real-time traffic analysis and packet logging on IP networks, which can work seamlessly on many different platforms such as Linux, Windows, MAC, and FreeBSD Detection and prevention system software. Snort, which is generally signature-based, can also perform protocol and anomaly analysis by using a set of paid or unpaid rules downloaded from www.snort.org and www.emergingTreats.com. They also have a flexible rule/policy setup language that allows users to write their own rules for attack detection, software protocol analysis, content scanning/mapping, buffer overflow, port scanning, operating system fingerprint test.

When Snort is used as an Intrusion Detection System (IDS), two network interface cards are usually used. One of the interfaces is used to listen to the network and remotely access Snort and configure Snort. The interface that listens to the network is generally not assigned an IP address but all the switch ports to which it is connected or mirrored. Snort will listen to all packets passing through the switch with this method.
Snort's architecture is based on performance, simplicity, and flexibility. It is built on four essential components: packet decoder, preprocessor, detection engine, and logging/alarm.

6.2 Suricate

Suricata is an open-source intrusion detection and prevention system distributed with a GPLv2 license. The first beta version was released in December 2009, and the first stable version was released in June 2010. Snort's support of the rules became effective soon after being accepted. Suricata has come up with significant innovations in attack detection. These are the new HTTP normalization tool called HTP library and developed by Ivan Ristic from the Suricata project team. The most important feature of this new tool that allows parsing HTTP traffic is "security-aware." It can capture various techniques that attackers can use to bypass intrusion detection systems. However, the library has different parses for request line, request header, URI, username, response line, server response line, and cookie, "basic" and "digest" authentication operations related to the HTTP protocol. Another essential feature of Suricata is its ability to support multi-threaded operations. For architects with multiple processor units, the packet processing is distributed in different departments with different threads. Each CPU unit acts as a separate machine running on a single processor. Thus, load balance is achieved, and performance is improved.

The characteristics of Suricata are as follows:

- It can be used in operation modes such as intrusion detection systems (IDS), intrusion prevention systems (IPS).
- It is possible to record the traffic in PCAP format and then analyze it offline by monitoring the network traffic. It also works in UNIX socket mode for the analysis of PCAP files.
- Linux, FreeBSD, OpenBSD, Mac OS X, Windows, and almost all operating systems can work.
- The configuration file is in YAML format, making it easy to understand. Many programming languages are supported. With Suricata 2.0 stable version, YAML file is divided into desired parts and called from the main file.
- The IPv6 protocol is fully supported.
- TCP sessions perform operations such as tracking the session from beginning to end, queuing the stream, etc. It also has a separate module for reassembling the shredded packages.

A study based on a comparison of Snort and Suricata found that both systems are sound [20].

6.3 BRO

Bro is an open-source, UNIX-based, BSD-distributed intrusion detection system, network analysis, and monitoring tool. It was first codified in 1995 by Vern Paxson, Lawrence Berkeley National Laboratory (LBNL). It was functionally developed in 1996 and announced in an article published in 1998. By 2003, the project was supported by the National Science Foundation (NSF) and is now being developed at the International Computer Science Institute (ICSI) in Berkeley.

Bro is a complex network traffic analysis tool, unlike the classical rule-based IDS. Traffic analysis covers security and includes performance analysis and networking solutions.

The characteristics of Bro are as follows;

- Linux, FreeBSD, MacOS and UNIX-based operating systems.
- It can analyze real-time or offline.
- It uses the library "libpcap" to capture packages.
- Bro users offer clusters ("Bro Clusters") wherever traffic is concentrated and distributed, such as universities, research laboratories, and large-scale businesses. Bro runs on different servers, and they can communicate between themselves.

9. Conclusion

IDS systems become the most critical security systems for e-government and e-business applications [21]. One of the ways to identify hackers is to use and tightly tune intrusion detection systems (IDSs), which try to detect or predict the probability of an attack in various ways, such as controlling the network traffic and detecting those trying to attack by creating too much traffic on the network [22]. Session Initiation Protocol (SIP) packet replay attack, SIP packet insertion attack, TLS connection reset attack, flood attacks, and fake message attacks are the most known DoS attacks. Using a SIP-supported firewall against such attacks provides detailed network analysis and prevents attacks by adding SIP-oriented rules to IDS and IPS devices. Multiple packets sent simultaneously can be detected with these systems, which can warn admins. Restriction can be in the form of not accepting packets from users outside the network, or it can be in the form of limiting the number of packets coming over a single IP. In addition, during the attack on the server, the attack can be detected manually by monitoring the network packets with tools like "*ngrep*". [23].

While the number of software vulnerabilities discovered and publicly disclosed by white hats or experts is increasing every year, only a small portion, if not all, of these vulnerabilities are used in real-world attacks. Due to constraints on time and qualified resources, organizations often look to ways to identify threatened vulnerabilities for patch prioritization. For this, robust threat intelligence is needed, which not every organization can do well and adequately [24]. Since we have found many zero-day exploits available in the exploit-DB database, it is highly recommended to tighten IDS and IPS tools and keep up to date with the latest vendor patches. Machine learning techniques are now widely used to perform effective attack detection, as attackers can quickly exploit techniques and zero-day vulnerabilities that bypass security measures and avoid direct detection. In this context, deep learning networks can play an essential role by analyzing network flows and classifying them as "normal" or "attacked". Various projects aim to design and implement tools for detecting zero-day threats (ZED-IDS, Zero Day Intrusion Detection System), and a deep learning architecture is used to detect DoS attacks [25, 26].

It is impossible to choose the most effective approach for IDS systems formed by very different methods. Still, the advantages and disadvantages of each IDS system are presented to the reader. It can be said that traces on Attack signature-based systems will increase in terms of the processing time in the future due to the day-to-day progress slowing down of such systems will be inevitable, and new investigations will eliminate this deficiency. More efficient signature-based intrusion detection systems should be developed. IDS and IPS systems should be used with firewall devices. These products are used together with the new generation Firewall devices, which enable the monitoring of the activity on the network and the analysis of the traffic to detect possible cyber-attacks, breaches, and threats. In this way, the performance problems that may arise are prevented and successful results by working more efficiently. Today, the complex structure of networks and the fact that they are connected to other networks, especially the internet, with many access points, make it easier for cyber attackers. It has become challenging to prevent complex network systems from increasing and developing attacks with technology development. It has become impossible to protect data and ensure information security with encryption or a stand-alone firewall.

Today, intrusion detection systems that apply artificial intelligence, machine learning, and data mining approaches are intensely confronted. Artificial intelligence plays a vital role in detecting intrusions and is widely considered the better way to adapt and build IDS. Nowadays, neural network algorithms have emerged as a new artificial intelligence technology applied to real-time problems [26]. As can be seen from the reviewed articles, researchers have concentrated on classifiers. There is also a question of how the intrusion detection systems run offline to show how they perform in real-time. A suggested way is to select real-time intrusion detection systems with faster and higher

detection rates by reducing the number of features by selecting only the critical components examined. In addition, more successful intrusion detection systems can be created by combining various categories of methods in the simplest terms using different 'fusion' approaches.

Another consequence of the studies examined is the need for up-to-date audit data sets. The data sets used in the studies are often very diverse and outdated. For this, it can be said that it is necessary to create quantitative and diversified data sets in terms of personal privacy. We believe that the methods that generate traffic data will be further developed to observe the real-time success of the intrusion detection systems presented in the literature and give us a more detailed interpretation of these systems.

Author's Contributions

Ahmet EFE: Guided the drafting and writing the manuscript, checked and finalized the work.
Irem Nur ABACI: Drafted preliminary content.

Ethics

There are no ethical issues after the publication of this manuscript.

References

[1]. Bahman Nikkhahan, Akbar Jangi Aghdam, and Sahar Sohrabi, "E-government security: A honeynet approach", *International Journal of Advanced Science and Technology Volume 5*, April, 2009 http://www.sersc.org/journals/IJAST/vol5/5.pdf

[2]. Niva Das, Tanmoy Sarkar, "Survey on Host and Network Based Intrusion Detection System" Department of Information Technology, University of Calcutta, Kolkata Email: niva.cu@gmail.com *Int. J. Advanced Networking and Applications Volume: 6* Issue: 2 Pages: 2266-2269 (2014) ISSN : 0975-0290

[3]. Yousef Farhaoui, Ahmed Asimi, "Creating a Complete Model of an Intrusion Detection System effective on the LAN" (IJACSA*) International Journal of Advanced Computer Science andApplications, Vol. 3*, No. 5, 2012

[4]. Zhitian Zhou, Congyang Hu, "Study on the E-government Security Risk Management", *International Journal of Computer Science and Network Security, VOL.8* No.5, May 2008 Manuscript received May 5, 2008 Manuscript revised May 20, 2008.

[5]. Wallner R., *Intrusion Detection Systems*, 2007, http://www.kiv.zcu.cz/~ledvina/DHT/tugraz/IDS.pdf

[6]. Young S. and Aitel D., *The hacker's handbook: the strategy behind breaking into and defending networks*. CRC Press, 2003.

[7]. Timm K., "Strategies to reduce false positives and false negatives in nids," *Tech. Rep*., Access Date 10 Oct, 2015.

[8]. Julisch K. and Dacier M., "Mining intrusion detection alarms for actionable knowledge," in *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining-KDD 02. Association for Computing Machinery* (ACM), 2002.

[9]. Chyssler T., Burschka S., Semling M., Lingvall T. and Burbeck K., "Alarm Reduction and Correlation in Intrusion Detection Systems".

[10]. Yang W., Wan W., Guo L. and Zhang L.J., "An Efficient Intrusion Detection Model Based on Fast Inductive Learning", *Internation Conference on Machine Learning and Cybernetics.*

[11]. Xuetao D., Chunfu J. and Fu Y., "A Typical Set Method of Intrusion Detection Technology Based on Computer Audit Data", *International Conference on Computational Intelligence and Security.*

[12]. Pikoulas J., Buchanan W., Mannion M. and Triantafylopoulos K., "An Intelligent Agent Security Intrusion System", *9th Annual IEEE International Conference and Workshop on the Engineering of Computer-Based Systems.*

[13]. Jemili F., Zaghdoud M. and Ben Ahmed M., "A Framework for an Adaptive Intrusion Detection System using Bayesian Network", *IEEE Intelligence and Security Informatics.*

[14]. B. Pahlevanzadeh and A. Samsudin, "Distributed Hierarchical IDS for MANET over AODV+", *IEEE Internatinal Conference on Telecommunications and Malaysia Interntional Conference on Communications.*

[15]. Bai Y. and Kobayashi H., "Intrusion Detection Systems: Technology and Development", *17th International Conference on Advanced Information Networking Applications.*

[16]. David J. Chaboya, Richard A. Raines, Rusty O. Baldwin, Barry E. Mullins, "Network Intrusion Detection: Automated and Manual Methods Prone to Attack and Evasion", *IEEE Security and Privacy.*

[17]. Silva M., Lopez D. and Abdelouahab Z., "A Remote IDS based on Multi Agent Systems, Web Services and MDA", *International Conference on Software Engineering Advances.*

[18]. Irfan Gul, M. Hussain, "Distributed Cloud Intrusion Detection Model" *International Journal of Advanced Science and Technology Vol. 34*, September, 2011 https://pdfs.semanticscholar.org/9e13/4e4ea8319869f95cc4efabc372fb5fbabe01.pdf

[19]. Hassen M. Alsafi, Wafaa Mustafa Abduallah, Al-Sakib Khan Pathan, IDPS: An Integrated Intrusion Handling Model for Cloud, *Computer Science, Networking and Internet Architecture*, March 2012, https://arxiv.org/abs/1203.3323

[20]. Chintan Kacha, Kirtee A. Shevade, "Comparison of Different Intrusion Detection and Prevention Systems" *International Journal of Emerging Technology and Advanced Engineering Volume 2*, Issue 12, December 2012) https://pdfs.semanticscholar.org/08d2/5088d72857dd05467a3689ac8a36e838e724.pdf

[21]. Mahmood Khalel Ibrahim et al, "Secure E-Government Framework: Design and Implementation*", IJCSET |May 2013 | Vol 3*, Issue 5, 186-193

[22]. Sajad Einy, Cemil Oz, Yahya Dorostkar Navaei, "The Anomaly- and Signature-Based IDS for Network Security Using Hybrid Inference Systems", *Mathematical Problems in Engineering, vol. 2021*, Article ID 6639714, 10 pages, 2021. https://doi.org/10.1155/2021/6639714

[23]. Yüksel, M. , Öztürk, N. "SIP Saldırıları ve Güvenlik Yöntemleri" . *Bilişim Teknolojileri Dergisi 10* (2017): 301-310 https://dergipark.org.tr/tr/pub/gazibtd/issue/30647/331042

[24]. Almukaynizi M., Nunes E., Dharaiya K., Senguttuvan M., Shakarian J., Shakarian P. (2019) Patch Before Exploited: An Approach to Identify Targeted Software Vulnerabilities. In: Sikos L. (eds) *AI in Cybersecurity. Intelligent Systems Reference Library, vol 151. Springer, Cham.* https://doi.org/10.1007/978-3-319-98842-9_4

[25]. Catillo, Marta, Rak, Massimiliano, and Villano, Umberto. 'Discovery of DoS Attacks by the ZED-IDS Anomaly Detector'. 1 Jan. 2019 : 349 – 365. *Journal of High Speed Networks*, DOI: 10.3233/jhs-190620

[26]. V. Kanimozhi, T. Prem Jacob, Artificial Intelligence based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing, *ICT Express, Volume 5*, Issue 3, 2019, Pages 211-214, ISSN 2405-9595, https://doi.org/10.1016/j.icte.2019.03.003.