Global Journal of Engineering and Technology Advances

eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(Review Article)

Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)

Safana Hyder Abbas *, Wedad Abdul Khuder Naser and Amal Abbas Kadhim

Department of Computer Science, University of Al-Mustansirihya, Baghdad, Iraq.

Global Journal of Engineering and Technology Advances, 2023, 14(02), 155–158

Publication history: Received on 02 January 2023; revised on 21 February 2023; accepted on 23 February 2023

Article DOI: https://doi.org/10.30574/gjeta.2023.14.2.0031

Abstract

Intrusion detection system (IDS) is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies. An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. If anomaly traffic pass through the network IDS would generate a false positive which means it only detects the malicious traffic, takes no action and generates only alerts but IPS detects the malicious traffic or suspicious activity, takes the actions like terminate, block or drop the connections. This paper provides an explanation of network intrusion, detection, and prevention to overcome them.

Keywords: Intrusion; Security; Attacks; IDS; IPS

1. Introduction

The IDS is a method that determines if there are any threats caused by intrusions on the system throughout the observations of the network traffic. It is available around the clock to generate information regarding the state of the system, monitor the activities of the users, and provide reports to a management station [1].

The purpose of IDS is to find different types of malware activities that are dangerous for computers and devices. Such activities include: network attacks against vulnerable services, attacks against privilege escalation, unauthorized access to sensitive files as well as the actions of malware (viruses, Trojans and worms) [2].

Intrusion prevention system (IPS) is the process of both detecting intrusion activities or threats and managing responsive actions on those detected intrusions and threats throughout the network. IPS are monitoring real time packet traffic with malicious activities or which match specific profiles and will trigger the generation of alerts and it can drop, block that traffic in real time pass through in network. The mainly IPS counter measures is to stop an attack in progress [3].

2. IDS/IPS Security

Some organizations use firewalls as well as routers along with IPS/IDS. Basically the difference between both is that firewall only checks IP address and port number. By using port number and IP address it blocks the traffic. It uses some signatures for detection; if packet meets the criteria or rules that are set in signatures it simply forward that packet otherwise block that packet.

[*] Corresponding author: Safana Hyder Abbas

Firewall is the first line which can protect our net-work against the intruders. It can detect only limited attacks. So we use IDS/IPS in between front end firewall and back end firewall which can detect and prevent the internal network traffic from the attacks. It can placed IPS/IDS in between that port and web server by comparing the traffic with the internally set signatures. So IDS/IPS provides an extra layer of protection for the traffic against internet accessible web servers [4].

3. Intrusion Detection Systems

IDS, analyze network traffic and generate alerts when malicious activity is discovered. They are generally able to reset TCP connections by issuing specially crafted packets after an attack begins and some are even able to interface with firewall systems to re-write firewall rulesets on the fly.

Intrusion detection systems are classified into two general types known as signature based and heuristic based. IDSs that operate on a single workstation are known as host intrusion detection system (HIDS), while those that operate as stand-alone devices on a network are known as NIDS. HIDS monitor traffic on its host machine by utilizing the resources of its host to detect attacks. NIDS operate as a stand-alone device that monitors traffic on the network to detect attacks. NIDS come in two general forms; signature based NIDS and heuristic based NIDS. These two types of NIDS provide a varying degree [5].

There are three different detection types for IDS: Misuse Detection, Anomaly Detection, and Hybrid detection:

Misuse detection, also known as signature detection, searches for known patterns of intrusion in the network or in the host. Each attack has a specific signature, for instance, it can be the payload of the packet, the source IP address, or a specific header. The IDS can raise an alarm if it detects an attack that has one of the signatures listed in the list of known signatures of the IDS. The advantage of this approach is its high accuracy to detect known attacks. However, its weakness is that it is inefficient against unknown or zero-day (never seen before attack) patterns.

Anomaly detection defines a normal state of the network or the host, called a baseline, and any deviation from this baseline is reported as a potential attack. For instance, anomaly-based IDS can create a baseline based on the common network traffic such as the services provided by each host, the services used by each host and the volume of activity during the day. Thus, if an attacker accesses an internal resource at midnight, and if in the baseline there should be almost no activity at midnight, then the IDS will raise an alarm. The advantage of anomaly detection is its flexibility to find unknown intrusion attacks. However, in most cases it is difficult to precisely define what the baseline of a network is, thus, the false detection rate of these techniques can be high.

Hybrid detection combines both of the aforementioned detections. Generally, they have a lower false detection rate than anomaly techniques and can discover new attacks [5].

4. Intrusion prevention systems

Intrusion Prevention Systems (IPSs) have become widely recognized as a powerful tool and an important element of IT security safeguards. An IPS is any device that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful. IPS technologies are differentiated from IDS technologies by one characteristic. IPS technologies can respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which can be divided into the following groups.

4.1. Response Techniques of IPS

IPS stops the attack itself. It can terminate the network connection or user session that is being used for the attack, and block access to the target from the offending user account, IP address, or other attacker's attribute. IPS can change the security environment. The IPS could change the configuration of other security controls to disrupt an attack. The IPS changes the attack’s content. IPS technologies can remove or replace malicious portions of an attack to make it benign.

4.2. Approaches to Intrusion Prevention Systems

There are different types of approaches is used in the IPS to secure the network.

- Signature-Based IPS: It is commonly used by many IPS solutions. Signatures are added to the devices that identify a pattern that the most common attacks present. That's why it is also known as pattern matching. These signatures can be added, tuned, and updated to deal with the new attacks.
- Anomaly-Based IPS: It is also called as profile-based. It attempts to discover activity that deviates from what an engineer defines as normal activity. Anomaly-based approach can be statistical anomaly detection and non-statistical anomaly detection. Policy-Based IPS: It is more concerned with enforcing the security policy of the organization. Alarms are triggered if activities are detected that violate the security policy coded by the organization. With this type approaches security policy is written into the IPS device.
- Protocol-Analysis-Based IPS: Is similar to signature based approach. Most signatures examine common settings, but the protocol analysis -based approach can do much deeper packet inspection and is more flexible in finding some types of attacks [6].

4.3. IPS technologies

- Network-based IPS (NIPS) monitors traffic in the network and blocks suspicious data stream.
- Wireless Intrusion Prevention Systems (WIPS) monitor actions in the wireless networks. Commonly, it detects wrong configured wireless access points, man-in-the-middle attacks, Mac addresses spoofing.
- Network Behavior Analysis (NBA) analyzes network traffic and looks for untypical streams, such as DoS and DDoS attacks.
- Host-based Intrusion Prevention (HIPS) is resident program, it detects suspicious actions on the computer [2].

5. Conclusion

IPS and IDS are foundation of technology that tracks, monitors the traffic across the network, identifies the suspected traffic, blocks and takes the necessary actions by informing the administrator.

The main difference between intrusion detection systems (IDS) and intrusion prevention systems (IPS) is that IDS are monitoring systems and IPS are control systems. IDS won't alter network traffic while IPS prevents packets from delivering based on the contents of the packet, similar to how a firewall prevents traffic by IP address.

IDS are used to monitor networks and send alerts when suspicious activity on a system or network is detected while an IPS reacts to cyberattacks in real-time with the goal of preventing them from reaching targeted systems and networks.

Compliance with ethical standards

Acknowledgments

The authors would like to thank the Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad, Iraq for supporting this work.

Disclosure of conflict of interest

All authors declare that they have no conflict of interest.

References

[1] Sheikh Tahir Bakhsh1, Saleh Alghamdi1, Rayan A Alsemmeari1 and Syed Raheel Hassan, "An adaptive intrusion detection and prevention system for Internet of Things", International Journal of Distributed Sensor Networks 2019, Vol. 15(11).

[2] Bezborodov Sergey," Intrusion Detection Systems and Intrusion Prevention System with Snort provided by Security Onion", Bachelor's Thesis Information Technology, 06.05.2016.

[3] Asmaa Shaker Ashoor, Sharad Damodar Gore," Difference between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)", Conference Paper, 10 May 2019 on Research Gate.

[4] Kanika," Intrusion Detection System and Intrusion Prevention System – A Review Study", International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August, 2013.

[5] Patrick Vanin , Thomas Newe , , Lubna Luxmi Dhirani , Eoin O'Connell , Donna O'Shea ,Brian Lee and Muzaffar R," Review: A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning", Applied science, 2022, 12, 11752. https://doi.org/10.3390/app122211752.

[6] K.C. Nalavadeand B.B. Meshram," Comparative Study of IDS and IPS", BIOINFO Computer Engineering Volume 1, Issue 1, 2011, pp-01-04