Intrusion Detection Systems

Esad Engin Işık
Computer Engineering
Yildiz Technical University
Istanbul, Turkey
engin.isik1@std.yildiz.edu.tr

Emir Kerem Öztürk
Computer Engineering
Yildiz Technical University
Istanbul, Turkey
kerem.ozturk @std.yildiz.edu.tr

Atahan Uz
Computer Engineering.
Yildiz Technical University
Istanbul, Turkey
atahan.uz@std.yildiz.edu.tr

Şeyda Şeyma Balcı
Computer Engineering
Yildiz Technical University
Istanbul, Turkey
seyma.balci @std.yildiz.edu.tr

***Abstract*— Intrusion Detection Systems (IDS) are critical components in modern cybersecurity infrastructure, specifically designed to monitor network traffic, examine the activities of the system it is integrated in and identify potential threats with real-time alerts and reports. Computer networks existed without IDSs in the past using different algorithms and security measures to keep precious data safe, from administrators analyzing the network log manually to antivirus software and Firewall technologies yet it was almost never sufficient. This report provides an overview of IDS, including its types, methods, evasion techniques, and placement strategies. We analyze the benefits and problems associated with IDS to provide a comprehensive understanding of the very important role that it has in protecting day to day networks, offering advice on their functional mechanisms and their effort to counteract always advancing cyber threats.**

***Index Terms*— Intrusion Detection System, Network Monitoring, Network Security**

I. Introduction

An Intrusion Detection System (IDS) is a security mechanism that is used to monitor either an electronic device or a networks traffic for suspicious activity and potential threats so they can be detected early before they become an issue and be dealt with [1] . We can split Intrusion Detection Systems into multiple types, they are as follows; Host-based IDS (HIDS) which are used for independent devices, Network-based (NIDS) which are used for computer networks and Hybrid IDS where HIDS and NIDS are used together for bigger projects. There are different detection methods that the IDSs use to get its job done, being signature-based and anomaly-based. IDS are often used in many real-life situations, including Universities, healthcare, government agencies, large enterprises and other places where computer networks need to be secure, playing an important role in protecting sensitive data, ensuring that the network works properly and maintaining integrity.

II. How IDS Works

Intrusion Detection Systems (IDS) does its work by monitoring network traffic and analyzing the patterns of the data packets that go through a network for irregular behavior. IDS starts by collecting data that includes log files, events that occur in the system and information [2] of the packet from the network and host activities. This makes sure that IDS knows what's happening in the system. After the collection of data, IDS analyzes it in real-time searching for patterns that would be a threat to the network. These threats could vary from unexpected logins to large data transfer. The IDS then compares the analyzed data to the pre-defined rules and signatures within the system. If the activity that's being compared matches the set of predefined rules, they become identified as suspicious, IDS quickly issues an alert. This alert can be different depending on the network it's in, from log entries to email notifications to SMS messages. The alert is always sent with a report to the system administrator or cybersecurity personal, informing them of the potential threat. Once the administrator is notified, they can act against the threat based on the report given. This study will also demonstrate how useful and precise IDS can work.

III. Types of Intrusion Detection Systems

The types of IDS can be categorized into three commonly used types: Host-based IDS (HIDS), Network-based IDS (NIDS) and Hybrid IDS. HIDS operate independently on each individual device such as laptops and computers or hosts, monitoring and analyzing malicious activity and threats that are internal. On the other hand, NIDS are designed for monitoring network traffic [3], with different methods of detecting malware. Their abilities to provide safety both to a devices and networks make them essential for modern companies and organizations which have complex network infrastructures with data that must be kept private. Hybrid IDS combines the features of previously talked about Intrusion Detection System types.

A. Host-based Intrusion Detection System (HIDS)

HIDS operates independently on each device within the network they are connected to, providing device-based monitoring to be able to detect threats and react to malicious activities. HIDS focuses on the security of hosts alone by examining the intra-activities. HIDS work by constantly monitoring multiple events on the host device, such as integrity of files, irregularities in the host behavior and system logs. HIDS also saves snapshots of files so it can compare them later once an attack is happening, comparing the files before and after an attack. The system prioritizes protecting databases, virtual machines and endpoints such as personal laptops, computers and mobile devices. They are very good at detecting threats that might go unnoticed by bigger NIDS, therefore making it healthy to have it on individual devices. HIDS is also efficient at preventing insider threats preventing malware injections from the inside. The alerts they generate for the system administrators are in depth and highly detailed, offering a broad explanation of the nature of the threat, everything that got affected by it, and the actions that should be taken.

B. Network-based Intrusion Detection System (NIDS)

Network-based Intrusion Detection Systems (NIDS) unlike the previous version HIDS, it monitors traffic throughout the entirety of the network it’s installed within. Making sure to keep organizational computer network infrastructure safe from cyber threats. NIDS work by collecting the data packets as they are travelling the network. It then inspects the captured packets to detect irregularities, which may imply that there has been a security breach. This analysis happens in real-time, and it gives NIDS the power to detect many types of cyber-attacks, including malware, attempts of unauthorized access to data and Denial of Service (DoS) where the attacker sends an overwhelming amount of traffic to the system. Primary advantage of NIDS being its ability to provide a very wide range view of the network activity, making it very useful for data centers [4] , enterprise networks and critical infrastructure environments. Moreover, NIDS are designed to be adjustable and adaptable depending on the size of the network they are being integrated to. They can be setup to monitor various network sections and a lot of protocols. Advanced NIDS even includes methods such as machine learning and artificial intelligence to make detecting advanced threats easier. Alerts they generate include details of the threat caught, affected network areas, and recommended solutions.

C. Hybrid Intrusion Detection System

Hybrid IDS combines the functions of both HIDS and NIDS, this combination provides a more comprehensive monitoring across devices and network traffic, offering the ability to examine the activities across both individual devices and the broader network that they are connected to [5] . By using the benefits of both HIDS and NIDS, Hybrid IDS is useful at detecting a much larger variety of potential threats. It is often employed in government, military, educational institutions, and large enterprises.

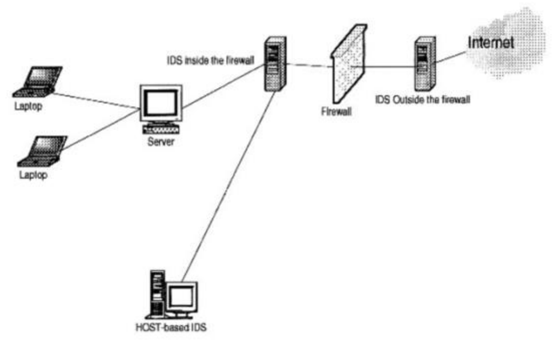

Figure 12.1 The Architecture of a Network-Based Intrusion Detection System

Categories	**HIDS**	**NIDS**
Type	Does not work in real time	Works in real time
Concern	HIDS is only concerned with a single host device	NIDS examines the activity and traffic of the entire network.
Installation Point	HIDS can be installed on any computer or server	NIDS is installed at specific points in the network system, such as routers or servers.
Execution Process	Works by comparing files to how they were before and after detecting malicious activity on the device.	NIDS works by examining data streams in real time and immediately reporting anything unusual.
Attack Responses	HIDS has more information about attacks because it is associated with system files and processes.	The larger the network, the less likely it is to be aware of attacks.
Installation	The installation process can be difficult as it needs to be installed on each host device.	There are few installation points
Response Time	Slow response time	Fast response time

Table 1

IV. Methods of Detection

A. Signature-based Method

Signature-based IDS monitors network packets for pre-determined attack patterns known as signatures. This method works by there being a database of signatures in the network that keeps potential attack patterns and threat behavior. The IDS then can compare the pre-determined signatures that are in the database with suspicious activity to see if there is an actual real-time threat in the network. Once a threat is spotted using this method, it is swiftly dealt with by creating an alert, writing a report and sending it to the administrator of the network for him to deal with it further. This method is highly effective for known attacks that have already been studied and added in as signatures. However, when it comes to cybersecurity, regular updates are necessary to make sure that the system can detect the latest threats. Even though signature-based method being an effective and strong system it also has its shortcomings which is its helplessness against threats that don't have existing signature in the IDS database and the fact that human maintenance is necessary to keep on analyzing the new threats. These vulnerabilities alone are enough for the usage of different methods.

B. Anomaly-based Method

The anomaly-based method for IDS compares the networks traffic to a baseline model which is the “normal” behavior for that specific network to identify potential threats. The baseline model is created by the network activity being observed and the patterns within being learned over a period. Anomaly-based IDS are essential when it comes to detecting previously unknown attacks because they focus on differences in the network with its predetermined baseline. This issue was the weakness of the signature-based method because it relied solely on attack signatures that the system already knows. Using [6] advanced machine learning algorithms, anomaly-based IDS can update itself and change baseline depending on what the new “normal” is for the network. This adaptability allows this method to detect and respond to evolving cyber threats in real-time.

When the IDS detects difference from the baseline, it flags these anomalies as suspicious activities. These anomalies are then examined to see if they are actual threats. For instance, lots of failed passwords could indicate a brute force attack. This type of method is almost essential in dynamic and complex networks where new attacks are very common. It is very good at identifying zero-day exploits (the name given to attacks that are being used for the first time).

V. Intrusion Detection System Evasion Techniques

IDS is a delicate system that provides security to many networks around the globe but there are still ways to go around it, although there are many ways to attack a network and new techniques constantly developing the most common ways attackers use are:

A. Fragmentation

When malicious data is being sent, instead of it being sent as one whole packet, fragmentation divides it into many tiny pieces making it harder to understand.

B. Encryption

Even though encryption is often used for protecting private data, attackers can also use it to encrypt the malicious packets.

C. Traffic Obfuscation

Overcomplicating the malicious messages.

D. Coordinated, low bandwidth attacks.

Even though encryption is often used for protecting private data. When attackers coordinate their attacks, and simultaneously strike a network to make it so IDS becomes overwhelmed and must deal with many threats at once.

VI. Placement of IDS

The ideal placement of IDS varies depending on the network's architecture [7]. There are several different approaches with the following being the most common.

A. IDS behind the Firewall

The firewall of the device or network becomes the first filter, dealing with loud internet noise and unwanted data. This allows the IDS to work productively focusing only on the important threats inside the network. It is both the most common and the most preferred way of placing the IDS. The only potential threat being that if the firewall breaks and a very strong malware enters the network, it can access the IDS and take it over without leaving time for a reaction.

B. IDS beyond the Firewall

The IDS acts as the first filter, instead of the firewall. Advantages here are the network load within the system is reduced because the threats are being analyzed and stopped outside and the IDS gets to work on solving the threats before they become an actual problem.

C. IDS within the Network

IDS is not close to the firewall but within the network. Mostly used to monitor internal network layers, though less commonly used.

VII. Benefits of IDS

IDS provides in depth defense for a working network, excels at detecting both external hackers and internal network-based threats, enhances network performance, very adaptable and integrating [8] it inside of a system of any size is not a problem, generates valuable reports on the attacks for system administrators to examine, it adds a protective layer on top of firewalls because firewalls are often not enough when the network is broad, and lastly helps reduce potential costs of data breaches and security incidents would cause by detecting the threat early and dealing with it.

VIII. Problems

The main weaknesses of IDS's are false positives and false negatives. An example for a false negative within the system would be the IDS not being able to recognize a threat and deeming it trustworthy. This could lead to many severe problems withing the organization that it happens to. To deal with this there are machine learning algorithms. On occasions IDS might have problems dealing with overwhelmingly busy networks because of the amount of load it needs to save, compare, analyze, detect and write reports for. It also requires monitoring the network it is installed within full-time to make sure the data is kept safe and systems like the "baseline" are always updated. IDSs [9] often struggle dealing with networks that use encryptions throughout all packages increasing the workload of the IDS by a ton. If the suspicious data is complex and massive it wastes time to analyze it.

IX. Conclusion

In conclusion, Intrusion Detection Systems are essential components within modern networks, providing the much necessary defense against a wide array of threats. The importance of the IDS cannot be underestimated, they are very important at all the areas they are deployed at. [10] They operate by continuously monitoring network traffic and system activity to detect and respond to security breaches, most of the time saving thousands of hours' worth of time by reacting to security breaches early. Their effectiveness lies in their ability to adapt to the always evolving cyber attack landscape. Using advanced technologies such as artificial intelligence and machine learning current Intrusion Detection System types can analyze massive amounts of data in real-time and give feedback on it, detecting even the most sophisticated threats. This adaptability is crucially important in the modern world where cyber attacks are a constant threat, and they are – just like the IDS [11] – always evolving and adapting. Despite their advantages they also have limitations such as their problems with false positives, which can overwhelm administrators with alerts that aren't actual threats. Additionally, less advanced Intrusion Detection System types require updates to remain effective as outdated systems fail to protect against new threats. However, the benefits of these systems significantly outweigh their shortcomings, being one of the only reliable ways of dealing with unwanted intrusion that doesn't require security teams to constantly check the network. The deployment of IDS is crucial throughout a nation, it is used within government sectors, military, healthcare, financial institutions, and large enterprises. These are sectors where just a small leak of private data could ruin lives. IDS perfectly provides an extra layer of security over the common defensive measures such as firewalls, and antivirus software. At the end IDS are indispensable tools when it comes to modern cybersecurity, offering significant protection and critical insight against all types of threats.

References

[1] Intrusion Detection System (IDS). Available: https://www.geeksforgeeks.org/intrusion-detection-system-ids/

[2] "Intrusion detection system," Wikipedia. Available: https://en.wikipedia.org/wiki/Intrusion_detection_system

[3] H. Kozushko, "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems," Sep. 11, 2003.

[4] P. Innella, "The Evolution of Intrusion Detection Systems," Digital Integrity, LLC, Nov. 16, 2001.

[5] D. E. Denning, "An intrusion-detection model," IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 222-232, Feb. 1987.

[6] A. S. Ashoor, "Importance of Intrusion Detection System," International Journal of Scientific & Engineering Research, vol. 2, no. 1, pp. 1, Jan. 2011.

[7] S. Vijayarani and M. S. Sylviaa, "Intrusion Detection System – A Study," International Journal of Security, Privacy and Trust Management (IJSPTM), vol. 4, no. 1, Feb. 2015.

[8] C. Lawrence, "IPS – The Future of Intrusion Detection," University of Auckland, Oct. 26, 2004.

[9] J. McHugh, "Intrusion and Intrusion Detection," International Journal of Information Security, vol. 1, pp. 14-35, 2001.

[10] R. Kemmerer and G. Vigna, "Intrusion Detection: A Brief History and Overview," IEEE Security and Privacy, pp. 27-30, 2002.

[11] T. Holland, "Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth," SANS Institute, GSEC Practical v1.4b, Option 1, 2004.