IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Intrusion Detection System And Its Challenges

Harmandeep Kaur (Assistant Professor Rayat Bahra University, Mohali)

Shyam Singh (Assistant Professor Rayat Bahra University, Mohali)

Abstract

An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat. In this paper we will consider the challenges of IDS that are false alarm rate, unbalanced datasets, and response time and various technique to overcome all these.

Keywords: intrusion detection, evaluation false alarm, unbalanced dataset, host based IDS, Hybrid IDS.

Introduction

The demand of an intrusion detection system in various applications has increased in the recent years since huge amount of data is available to be stored and processed every day. The networking systems are generating huge amount of data by monitoring the surroundings of applications in which they are deployed. Any kinds of suspecting behaviors are detected by the devices. Any kinds of vulnerabilities in any computer network can be found by an intruder that aims to harm the users using that device. For preventing the entry of intrusions, the best solution is to protect the system or its resources . Following are the important security perspectives to be considered to secure a computer system:

Confidentiality:The information can be accessed only by an authorized user.
Integrity: The information must not be affected by any vulnerability of system.•
Availability:By ensuring that the functioning of system is not degraded, authorized users must be provided access to the systems and its resource.

Any activity that attempts to trigger an event due to which the system's security is compromised is called as an intrusion. Either internally or externally, the intrusions might occur in any system. Any kind of illegal activity or fraud information that makes a computer hazardous can be considered as intrusion. In an intrusion detection system, it is possible to monitor and analyze episodes to be carried out within a computer network so that it becomes easy to recognize the security problems. This systems act as an alarm and any kinds of violations in the system are identified by it. Even if there are false messages in messages, mails or video sounds, they can be alerted by the systems. A tool that acts as a guard such that the system can be secured against any kinds of intrusions or attacks is called intrusion detection system. To check the attack scenarios and provide required support for defense management are the important objectives of IDS. Today, in networking, almost all the applications are using IDS systems.

Classification of Intrusion Detection Systems

Intrusion detection systems are designed to be deployed in different environments. And like many cyber security solutions, an IDS can either be host-based or network-based.

- **Host-Based IDS (HIDS):** A host-based IDS is deployed on a particular endpoint and designed to protect it against internal and external threats. Such an IDS may have the ability to monitor network traffic to and from the machine, observe running processes, and inspect the system's logs. A host-based IDS's visibility is limited to its host machine, decreasing the available context for decision-making, but has deep visibility into the host computer's internals.
- **Network-Based IDS (NIDS):** A network-based IDS solution is designed to monitor an entire protected network. It has visibility into all traffic flowing through the network and makes determinations based upon packet metadata and contents. This wider viewpoint provides more context and the ability to detect widespread threats; however, these systems lack visibility into the internals of the endpoints that they protect.
- **Protocol-based Intrusion Detection System (PIDS):** Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol. As HTTPS is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
- **Application Protocol-based Intrusion Detection System (APIDS):** An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.
- **Hybrid Intrusion Detection System:** Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system. The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

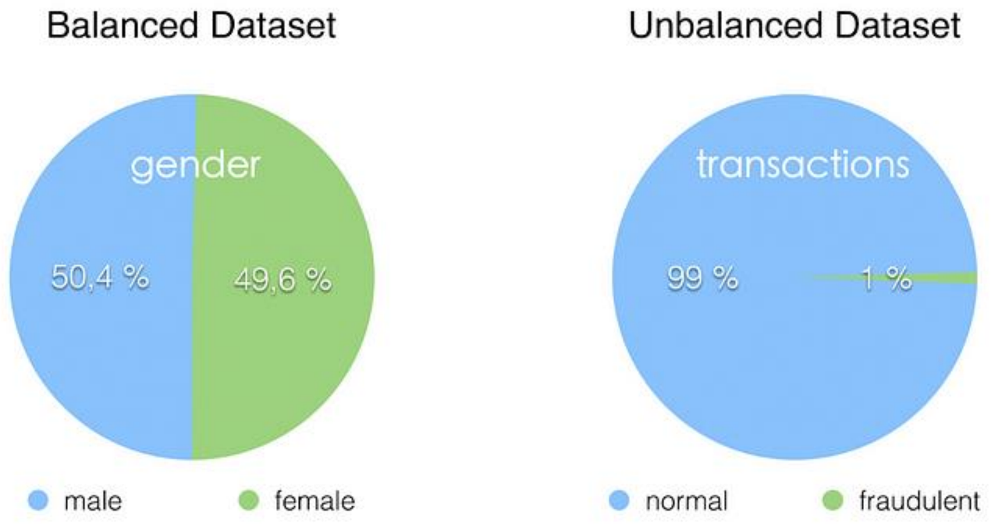
Challenges of intrusion detection systems

1) False alarm rate: - When a piece of security equipment warns you of a problem, this is known as a **false positive**. The problem is that the security device is malfunctioning. This is a positive. However, it's a false positive, meaning there was no issue.

These warnings are based on signatures if you receive a message from an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS). A piece of information that gone through the IPS that matches a signature and informs you that there was a match to that. In most cases, we have to rely on these signatures, so make sure you're using the most updated signatures to avoid false positives.

2) Unbalanced Dataset:- In simple terms, an unbalanced dataset is one in which the target variable has more observations in one specific class than the others.

For example, let's suppose that we have a dataset used to detect a fraudulent transaction. If we have a binary target variable (2 classes) — that's 1 when the transaction is fraudulent and 0 when it isn't — it's normal for less than 1% of the observations to belong to class 1 (fraud) than to class 0 (not fraud). In this case, we have a highly unbalanced dataset.



3) Response time:- An intrusion response system (IRS) is a critical part of the self-protecting system for ensuring appropriate responses are dispatched to react to protect the HIS and recover system performance back to normal. The tight interaction between the NFA module and the IRS module makes future attacks, which have similar signatures, less likely to succeed. The development of an autonomous IRS focuses on two key elements: configuring suitable responses and evaluating recommended responses dynamically.

Detection Method of IDS Deployment

Beyond their deployment location, IDS solutions also differ in how they identify potential intrusions:

- **Signature Detection:** Signature-based IDS solutions use fingerprints of known threats to identify them. Once malware or other malicious content has been identified, a signature is generated and added to the list used by the IDS solution to test incoming content. This enables an IDS to achieve a high threat detection rate with no false positives because all alerts are generated based upon detection of known-malicious content. However, a signature-based IDS is limited to detecting known threats and is blind to zero-day vulnerabilities.
- **Anomaly Detection:** Anomaly-based IDS solutions build a model of the “normal” behavior of the protected system. All future behavior is compared to this model, and any anomalies are labeled as potential threats and generate alerts. While this approach can detect novel or zero-day threats, the difficulty of building an accurate model of “normal” behavior means that these systems must balance false positives (incorrect alerts) with false negatives (missed detections).
- **Hybrid Detection:** A hybrid IDS uses both signature-based and anomaly-based detection. This enables it to detect more potential attacks with a lower error rate than using either system in isolation.

Conclusion

Intrusion detection systems represent a technology that has been with us for decades, with some of the first systems foundational outlines still present, in some way, in today's more modern solutions. While flawed and challenged by shortcomings in its detection methods and functionalities, the IDS remains an important part of any cyber security architecture. Just as with many security solutions and technologies, an IDS shouldn't be a simple "install and you're done" proposition, but should be fine-tuned and properly configured to differentiate normal traffic from that which is potentially malicious, and continuously updated to keep up with today's ever-evolving security threats.

References:

1.D.E.Denning, An intrusion-detection model, IEEE Trans software Eng SE-13(1987) 222–232.

2.M.Moradi,M.Zulkernne A neural network based System for intrusion detection and classification of attacks ,in IEEE international conference on advance in intelligent system Theory and application,2004.

3.Wang,X.Hong, R.R. Ren, T.Li, A real-time intrusion detection system based on PSO-SVM In The 2009 International Workshop on information security and applications,2009 .

4. Denning, D: An Intrusion-Detection Model. IEEE Transactions on Software Engineering 13(2),118-131(1986).

5.Janne Anttila", Intrusion Detection in Critical Ebusiness Environment", Presentation,2004.

6.DK.Müller", IDS - Systems of intrusion Detection, Left II ", July 2003, http://www.linuxfocus.org/Francais/July2003/article294.shtml