IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023

DOI: 10.17148/IJARCCE.2023.12212

Intrusion Detection and Prevention Systems: A Comparative Analysis of Techniques and Approaches

Dr.Achyutha Prasad N [1], Varshith Kumar [2], K Rachith [3], Shreyas S Rokhade [4], Shashank S [5]

Head of Dept.CSE, East West institute of Technology, Bangalore,India[1]

Bachelor Of Engineering, East West Institute of Technology, Bangalore, India[2,3,4,5]

Abstract: Intrusion detection and prevention systems (IDPS) are an essential tool in protecting modern networks against cyber threats. They monitor network traffic and detect malicious activity, such as malware infections, unauthorized access, and network intrusions. When an IDPS detects such activity, it can take a variety of actions to prevent or mitigate the threat. IDPS systems can be configured to operate at various points within a network, including at the perimeter, at key servers, or on individual devices, allowing for a multi-layered approach to security. There are several types of IDPS technologies available, including signature-based systems and anomalybased systems, which use machine learning to identify deviations from normal network behavior. IDPS systems are an important part of a comprehensive network security strategy, but they are not foolproof and must be carefully configured and maintained to ensure optimal performance. It is also important to use IDPS in conjunction with other security measures, such as firewalls and user training.

Keywords: SOC (Security Operation Center), IDPS (Intrusion Detection and Prevention System), IDS (Intrusion Detection System), NIC (Network Interface Controller), G-IDS (Generative adversarial network – IDS), CPS (cyber-physical system)

I. INTRODUCTION

An IDPS is a network security tool that monitors and analyzes network traffic for malicious activity or policy violations. It aims to detect and prevent unauthorized access, misuse, and other malicious activities on a network in real-time. IDPS is an essential component of a comprehensive network security strategy, as it helps organizations protect their sensitive data and systems from cyber threats. There are two main types of IDPS: network-based IDPS and host-based IDPS. Network-based IDPS monitors traffic on the network and looks for patterns that indicate an intrusion attempt. Host-based IDPS, on the other hand, monitors the activity on a specific host or device and looks for signs of an intrusion. Both types of IDPS use a combination of hardware and software to monitor network traffic and analyze it for suspicious activity.

IDPS uses a variety of techniques to detect and prevent intrusions, including signature-based detection, anomalybased detection, and behavior-based detection. Signature-based detection uses a database of known attack patterns or "signatures" to identify known threats. Anomaly-based detection looks for deviations from normal behavior, which could indicate an intrusion attempt. Behavior-based detection analyzes the behavior of the system or network to identify unusual activity. IDPS can be configured to alert security personnel or automatically respond to detected threats. For example, an IDPS may block an incoming connection or quarantine a file that has been identified as malicious. IDPS is often used in conjunction with other security measures, such as firewalls and antivirus software, to provide multiple layers of protection for a network.

One of the key benefits of IDPS is that it provides real-time protection against cyber threats. As IDPS continuously monitors network traffic, it can detect and prevent an intrusion as it is happening, rather than after the fact. This can help prevent significant damage to a network and the data it contains. IDPS also provides organizations with valuable insights into their network security posture. It can help identify vulnerabilities and potential areas of improvement in an organization's security practices. IDPS can also provide valuable data for forensic analysis in the event of a security breach.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023
DOI: 10.17148/IJARCCE.2023.12212

However, IDPS is not a foolproof solution for network security. It is only as effective as the rules and signatures configured to use, and it can be bypassed by sophisticated attackers. Additionally, IDPS can generate false positives, which can lead to false alarms and unnecessary work for security personnel. It is important for organizations to carefully configure and maintain their IDPS to ensure it is functioning effectively.

I. LITERATURE SURVEY

[1] A Raspberry Pi is a compact, low-cost computer, to advance the study of fundamental computer science in colleges and universities. It is still a portable, inexpensive Linux-based computer that can execute programs with low power consumption even though it has less processing power than a current computer.
It can perform a variety of functions, such as web browsing, playing video games, and developing home automation devices, and may be used as a typical laptop or desktop computer by plugging it into an output screen and using a mouse and keyboard to operate as normal. The Raspberry Pi is also frequently used in several projects in a variety of industries.

Making an IDS, a security tool for computers and networks that analyzes data and spots malicious behavior by collecting incoming and outgoing network traffic and applying predefined rules to attacks is one use for the Raspberry Pi. IDS systems can be either network-based (deployed on a physical network and intercepting all traffic sent to the network) or host-based (deployed on a single host machine). IDS systems can also be anomaly-based, which tracks network, host, and user behavior over time to provide data and notify the user when unexpected or abnormal traffic is discovered, or rule-based, which compares past data with present data to identify attacks.

The development of a honeypot, a type of decoy system used to entice attackers and gather data on the attack and the attacker, is another use for the Raspberry Pi. Honeypots are continuously monitored by an administrator and are set up to appear susceptible. Any contact with a honeypot is viewed suspiciously and is recorded for investigation. When it comes to fending off attacks and learning more about them, honeypots can be incredibly effective.

A packet analyzer, commonly referred to as a packet sniffer, is a device that can intercept and record network traffic data. Packet analyzers can be used for a number of things, such as identifying security risks, monitoring network usage, and diagnosing network problems. By employing a NIC in promiscuous mode, which enables the device to record all network data rather than just that intended for it, the Raspberry Pi can be used to build a packet analyzer. This can be helpful for locating and examining network activity as well as for spotting security issues.

[2] The G-IDS framework is an IDS that uses machine learning to identify and classify different kinds of hacks in a CPS. The database module, the deep learning model module, the data synthesis module, and the controller module make up the framework's four primary modules.

Data collection and storage for the IDS are the responsibility of the DM. A database and a data collector make up the system. By utilizing a packet capture application to gather network packets, the DC is able to record actual network data. Before saving the packets in the DB, the DC preprocesses them by performing tasks including label encoding, feature scaling, and feature extraction. The database maintains the gathered information together with labels identifying the data type and flags identifying the status of data.

The machine learning models used by the IDS are trained and assessed by the DLM. It includes a PM and an HDLM. CNN and LSTM networks are combined to create the HDLM. It is trained using a hybrid database with both real and made-up data. The performance of the HDLM is assessed using the PM, which also identifies any weak labels (i.e., labels with low performance).

The DSM is in charge of compiling data to increase the training dataset for the IDS. It is made up of a discriminator network and a generating network. A GAN is used to train the G and D to create new data samples that are identical to the original data but do not include any sensitive information. A synthetic flag is then added to the database along with the synthesized data.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023
DOI: 10.17148/IJARCCE.2023.12212

Controlling the IDS's overall performance is under the purview of the CM. It keeps an eye on the PM and spots any shoddy labeling. The DSM is then given the weak labels to produce synthetic data in order to enhance the performance of the HDLM on those labels. Additionally, the CM manages the HDLM's training on the hybrid database and updates the PM following each training iteration. If the HDLM's PM on the hybrid database gets better, the CM accepts the synthetic data and retrains the HDLM using the new hybrid database. The HDLM is retrained using the original dataset if the PM does not improve after using the synthetic data.

[3] Fail2ban is a security tool that helps protect servers from malicious attacks by detecting and blocking them. It uses the IDPS method, which combines an IDS with a firewall, to monitor and block attacks on servers. By default, fail2ban can only be used on one server and cannot be used in conjunction with other servers. However, in this research, the authors propose a system where fail2ban can be used on multiple servers in a network to share attack information and block attackers across the network.

The system works by using a star topology, where one central terminal is connected to all other servers. When an attacker tries to perform a brute force attack on a server, the server running the fail2ban service will monitor the activity and block the attacker's IP address. The attack information will then be sent to a collector database, where it is stored and can be accessed by other servers in the network. These other servers can then use the attack information to block the attacker's IP address and prevent future attacks. An administrator can also monitor attacks in real-time on a website used for monitoring.
The authors outline the steps for installing and configuring fail2ban on the servers, including setting up rules for blocking attacks and configuring ban actions to send attack information to the collector database. They also describe the process for retrieving attack information from the database and using it to block attackers on other servers. The authors implemented this system and tested it, finding that it was successful in detecting and blocking attacks on the servers. Overall, the authors' research provides a solution for using fail2ban to protect multiple servers in a network from malicious attacks. By sharing attack information and using it to block attackers across the network, servers can be more effectively protected from threats.

[4] The research presents a conceptual machine learning-based IDS for detecting and classifying attacks on a network. The IDS uses a Raspberry Pi computer with a Raspbian operating system and Python programming to detect and classify attack patterns using machine learning techniques and monitor port scans for intruder activity on the network. The IDS classifies intruders into three lists based on the behavior and stores logs of their activity in a database.

The IDS begins by processing data to understand the signatures of existing behavior on the network. This involves training and testing data to develop a classifier that can identify anomalies and classify them into normal or anomaly behavior. Anomaly behavior is then further classified into subtypes, such as R2L and U2R, using a K-Means clustering approach.

The IDS also uses a Nmap scanner to track hosts connected to the local network and alert and block intruders when they attempt to access a host's IP address. Intruders who attempt to access the host's IP less than five times are added to a Graylist, while those who attempt it more than five times are added to a Blacklist, and all traces of them are removed from the system.

Overall, this research proposes a machine learning-based IDS that is able to detect and classify attacks on a network, monitor and block intruder activity, and store logs of intrusions in a database. It uses a combination of training and testing data, K-Means clustering, and a Nmap scanner to achieve these goals.

II. CONCLUSION

The Adaptable Plug and Play Security Operations Center has proposed a new Intrusion Detection and Prevention System (IDPS) that utilizes programmable plugins. This modular and scalable system is designed to easily adapt to the changing needs of the security operations center and effectively detect and prevent various attacks, including denial-of-service, viruses, and worms. While it has been tested and proven effective, IDPS systems require careful configuration and monitoring to avoid false positives and should be used as part of a comprehensive security strategy.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023
DOI: 10.17148/IJARCCE.2023.12212

ACKNOWLEDGMENT

The sense of accomplishment and euphoria that comes with completing a task would be incomplete without mentioning the people who make it possible, whose constant guidance and encouragement propel our efforts to success. We would like to express our heartfelt gratitude to **Dr. Achyutha Prasad N**, Professor and (Head of the Department of Computer Science and Engineering, East West Institute of Technology), Bangalore, for his encouragement and guidance, as well as his timely inspection and guidance throughout the process. We also want to thank the members of the Computer Science and Engineering faculty, whose suggestions helped us overcome many seemingly insurmountable obstacles.

REFERENCES

[1]. [1]. Shyava Tripathi and Rishi Kumar B." Raspberry Pi as an Intrusion Detection System, a Honeypot and a Packet Analyzer" 978-1-5386-7709-4/18/$31.00_c 2018 IEEE.
[2]. [2]. Md Hasan Shahriar, Nur Imtiazul Haque, Mohammad Ashiqur Rahman, and Miguel Alonso Jr. "G-IDS:
[3]. Generative Adversarial Networks Assisted Intrusion Detection System", 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC) 978-1-7281-7303-0/20/$31.00 ©2020 IEEEDOI 10.1109/COMPSAC48688.2020.0-218.
[4]. [3]. Mohammad Idhom, Henni Endah Wahanani and Akhmad Fauzi. "Network Security System on Multiple Servers Against Brute Force Attacks" 2020 6th Information Technology International Seminar (ITIS) | 978-1-72817726-7/20/$31.00 ©2020 IEEE | DOI: 10.1109/ITIS50118.2020.9321108.
[5]. [4]. Sumanth R and Bhanu K.N, "Raspberry Pi Based Intrusion Detection System Using K-Means Clustering Algorithm" IEEE Xplore Part Number: CFP20N67-ART; ISBN: 978-1-7281-5374-2.