6-2 Project Two: IDS Analysis Paper

Joshua Merren

Southern New Hampshire University

CYB-310-13414-M01 Network Defense

Professor Megan Buckner

9 October 2024

Intrusion Detection Systems (IDS) play a crucial role in protecting the confidentiality of information in network environments. Among the various types of IDS, Signature-based IDS (SIDS) is particularly effective. They utilize pattern-matching techniques to detect known threats by comparing network data against a database of previously identified intrusion signatures (Khraisat et al., 2019). This method is highly reliable for detecting known malware and unauthorized access attempts, making it essential for safeguarding sensitive data. However, the effectiveness of SIDS hinges on regularly updating the quality and currency of the signature database to include new and evolving threat patterns. This proactive updating is crucial because cyber threats continually change, and new attacks are constantly being developed (Creech & Hu, 2013). By keeping the database current, organizations can ensure that their SIDS are prepared to defend against the latest threats, thereby maintaining the confidentiality of their networks. Integrating these systems with other security measures is essential for a more comprehensive defense strategy. Integrating SIDS with other security components, such as firewalls and anomaly-based IDS, can provide a layered security approach that enhances overall network protection (Butun et al., 2014). Through diligent monitoring and updating, SIDS can effectively prevent unauthorized access and protect sensitive information from being exposed.

An IDS detects a range of indicators signaling the presence of malware, which can threaten data integrity within a system. These indicators include unusual data transmissions, unauthorized changes to system files, and anomalous application behaviors (Butun et al., 2014). For example, an anomaly-based IDS (AIDS) monitors deviations from standard behavior patterns established through statistical, knowledge-based, or machine-learning methods and flags these as potential security issues (Alazab et al., 2012). This capability is vital for detecting malware that can alter, corrupt, or delete data, compromising its accuracy and reliability. Such early detection is crucial for initiating quick corrective actions to prevent further damage and maintain the integrity of the system's data. Moreover, maintaining data integrity is not just about avoiding data tampering but also about ensuring the data remains consistent and accurate across all system exchanges. IDS systems help accomplish this by continuously monitoring the network and systems for any signs of compromise. Furthermore, integrating IDS with comprehensive logging and monitoring tools can help give a more detailed insight into the network's security status, enabling more precise detections and quicker response times. Regular updates to the IDS algorithms and databases are also essential to keep up with the evolving nature of malware threats, ensuring that the systems can detect new attacks that could affect data integrity.

An IDS plays a pivotal role in detecting threats that could lead to a loss of availability, such as DDoS attacks, which aim to overwhelm systems and make them unavailable to users (Creech & Hu, 2013). These systems monitor network traffic and analyze it for patterns that deviate from the norm, which might indicate an ongoing attack. Early detection is critical to mitigating these attacks before they can cause significant disruption. For instance, Network-based IDS (NIDS) is specifically designed to monitor large volumes of traffic at various strategic points in the network to detect potential threats from external sources (Butun et al., 2014). By identifying these threats early, NIDS helps organizations respond quickly to prevent or minimize downtime. Moreover, using Host-based IDS (HIDS) complements NIDS by monitoring specific computers or devices on the network, providing a more granular level of insight into individual system behaviors that could indicate a potential loss of availability. Combining both types of IDS offers a comprehensive monitoring solution that enhances the organization's ability to maintain continuous service availability. Employing redundancy and failover mechanisms alongside IDS can further bolster the network's resilience against availability threats. Implementing these technologies and strategies ensures that services remain available and operational, even in the face of attempts to disrupt them.

Consider a company named "GreenTech Innovations," which specializes in renewable energy solutions and operates from two buildings: the Research Lab and the Corporate Office. The company employs about 400 staff, including researchers, engineers, and administrative personnel. It handles sensitive data such as proprietary technology designs, financial records, and personal employee information. The Research Lab focuses on developing new technologies. It thus holds critical technical data and intellectual property, while the Corporate Office manages the operational aspects of the business, including employee records and financial data. GreenTech requires a robust and tailored security strategy to protect these diverse data assets across different locations. This strategy must account for the various types of data and their respective security requirements, equipping both buildings with appropriate IDS solutions tailored to their specific needs.

To protect GreenTech Innovations, you must optimize each component of the IDS for its specific environment. The Anomaly-based IDS installed in the Research Lab should be configured with advanced machine-learning algorithms to learn from ongoing activities and adapt to new, legitimate research behaviors without flagging them as false positives. This adaptability is vital in such a dynamic setting where new data patterns constantly emerge as a part of innovative processes (Alazab et al., 2012). Meanwhile, it would help if you equipped the corporate office with the signature-based IDS with the latest virus definitions and intrusion signatures updates. This ensures that even the most recently identified threats are known to the system, enabling it to protect against a wide range of attacks effectively. Regular updates and maintenance are critical as the threat landscape evolves rapidly, and staying ahead of potential attackers is key to safeguarding sensitive personal and financial information (Khraisat et al., 2019). Additionally, integrating these systems with a comprehensive incident response plan that includes automated processes and human oversight can significantly enhance their effectiveness. Automated processes ensure rapid initial response to potential threats, while human oversight provides deeper analysis and decision-making capabilities crucial for complex or subtle security incidents. This double approach alerts staff to threats and provides actionable intelligence to fortify the company's defenses against future attacks. These enhancements and strategic implementations ensure that both components of the IDS work synergistically to provide robust security across all sectors of GreenTech Innovations, adapting to the unique challenges posed by each environment within the company.

References

Alazab, M., Venkatraman, S., Watters, P., Alazab, M., & Alazab, A. (2012). Cybercrime: the case of obfuscated malware. In *Springer eBooks* (pp. 204–211). https://doi.org/10.1007/978-3-642-33448-1_28

Butun, I., Jr., Morgera, D., & Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. In IEEE, *IEEE Communications Surveys & Tutorials* (Vol. 16, Issue 1, pp. 266–267) [Journal-article]. https://doi.org/10.1109/SURV.2013.050113.00191

Creech, G., & Hu, J. (2013). A semantic approach to Host-Based intrusion detection systems using contiguousand discontiguous system call patterns. *IEEE Transactions on Computers*, *63*(4), 807–819. https://doi.org/10.1109/tc.2013.13

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2(1). https://doi.org/10.1186/s42400-019-0038-7