Journal of Science, Innovation and Creativity
Vol. 2 No. 1 (2023): ISSN (Online): 2958-454X
DOI: https://doi.org/10.58721/jsic.v2i1.287
Enhancing Cybersecurity: Smart Intrusion Detection in File Server SYSTEMS

Enhancing Cybersecurity: Smart Intrusion Detection in File Server SYSTEMS

Chrispus Alukwe
Kabarak University, Kenya

Article History
Received: 2023-06-06
Revised: 2023-07-12
Accepted: 2023-07-18
Published: 2023-08-17

Keywords
Cyber security
Cybercrime
Cyber-attacks
Cybercriminals
Cloud computing

How to cite:
Alukwe, C. (2023). Enhancing Cybersecurity: Smart Intrusion Detection in File Server SYSTEMS. *Journal of Science, Innovation and Creativity*, *2*(1), 1-6.

Abstract
System security is a major challenge worldwide, which has led to the increasing implementation of security surveillance systems in the public and private sectors. Likewise, it is inevitable to secure server-based systems that store vast amounts of sensitive data that is accessed from time to time. Intrusion Detection Systems (IDS) use metrics to detect anomalous activity on computers and computer networks. Modern detection algorithms try to reach detection metrics by acting as an antivirus. This is not enough, the need to explore more controlled, porous and more secure systems is inevitable, hence this research. Therefore, this study's main objective is to develop smart intrusion detection systems for file servers and client machines that can be used within any networked environment. A qualitative research methodology was employed in the study. The sources of information included four databases: SpringerOpen, EBSCO, Google Scholar, and Direct Science. The key findings of the study are that cyber-attacks and threats are increasing, and new strategies are needed to handle them because the current intrusion detection systems experience challenges and are unable to detect malware. Intrusion detection systems are the next-generation protection, which offers the visibility to identify advanced threats within legitimate content, even authorized applications and trusted sources. Organizations are recommended to implement smart IDSs in front of file server systems and behind the firewall to ensure all malware is filtered.

Introduction

Computer security has grown increasingly important due to the rapid evolution of cloud computing and high internet usage (Khraisat et al., 2019). Cyber-attacks and vulnerabilities continue to become more sophisticated due to the rapid development of technology. This has made it difficult for individuals and organizations to accurately identify intrusions. An intrusion detection system refers to a computer system that detects inappropriate, unusual, erroneous, or suspicious activities on a server-based system and networks. In other words, IDS checks for suspicious activities or policy violations and produces reports to protect the network (Jabez & Muthukumar, 2015). The number of cybercriminals has increased throughout the world and they aim to identify new targets, illegitimately acquire funds, and steal confidential information (Khraisat et al., 2019). The rate of cybercrime has increased due to the high reliance on internet and network services. Currently, novel attack techniques are perceived in organisations regularly. Thus, a new strategy is needed to control and monitor malicious activities that might interfere with network and computer systems. New techniques such as intrusion detection systems are essential to manage cybercrimes and threats, which are becoming common in the organisation.

Cloud computing and network security have fully taken hold and are now widely used worldwide, where network security professionals are studying how resources are compromised. The management and use of cloud computing services introduce new security challenges and attacks that cannot be solved with traditional pull network information security approaches known to attackers (George et al., 2012). The reliability of security services, including availability, confidentiality, and integrity, could be compromised if intrusions are not prevented. Therefore, it is important to develop smart intrusion detection systems for file servers and client machines that can be used within any networked environment, which is the study's main objective.

Methods

The study employed a qualitative research methodology, which involved reviewing past studies or articles related to the study topic. A qualitative methodology allows researchers to gather and analyse non-numerical data, including audio, text, and video (Aspers & Corte, 2019). It was adopted in this research because it enabled the researcher to obtain answers to questions that were difficult to put into numbers to comprehend the research phenomena. It also offered an in-depth comprehension of different types of malware and how smart IDS can be utilised to identify and prevent malicious software from interfering with the functioning of computer and network systems.

The sources of information included four databases: SpringerOpen, EBSCO, Google Scholar, and Direct Science. Several keywords, such as intrusion detection systems, cybercrime, malware, cyber security, and cloud computing, were used alone and in combination to search for relevant information from the databases. A total of 252 articles related to smart intrusion detection systems and cyber security were found. However, only 13 articles were relevant and used in this study. The eligibility criteria for articles were that the articles must be peer-reviewed and should be relevant to the study topic.

Results

The study results have shown that cyber-attacks and threats are increasing, and new strategies are needed to handle them because the current intrusion detection systems experience challenges and cannot detect malware. One of the major issues with this old mechanism is that it generates numerous false alerts, which the research journal is to table factual active concepts that will generate valid alerts of IDS while ensuring their reliability. Research has revealed that it is impossible to implement sufficient or too much security due to the increased use of the Internet to access different online services (Liao et al., 2013). Nevertheless, organisations should implement reliable security that does not compromise the system or network performance. Intrusion detection systems are essential to maintain information integrity, confidentiality, and availability, which is a significant asset in an organisation. They offer a second security layer and supplement other defence techniques like access control and authentication (Khraisat et al., 2019. Organisations should be aware of their actual needs and the existing infrastructure before implementing an IDS.

Research has indicated that the development of IDSs has become challenging due to the evolution of cyber-attacks and the introduction of malicious software. Currently, malicious software developers employ sophisticated strategies to conceal information to avoid being detected by an intrusion detection system (Canavan, 2001). Current security trends are already known to most attackers; some are the inventors. The carriers used today are becoming more sophisticated, and experiences of continuous data loss result in significant capital losses. As a result, it has become hard to detect malicious software (Khraisat et al., 2019). Behind the scenes, phishers and hackers routinely remain anonymous, attack systems and go undetected.

Digital forensics has yet to be perfected to link incidents to exceptional analytics that can convince investors to opt for a system where security can be managed at the vendor level (Nicholas et al., 2000). Cyber-attacks continue to be a lucrative business for criminals, where the sophisticated weapons of criminals keep growing, trying to exploit any vulnerabilities in an open system to commit fraudulent activities. It is important to expose a design and show an escalation of sample smart IDS to capture alerts generated by conventional intrusion detection systems while investigating whether such alerts can be valid or false, considering that such attacks on the host computers can be vulnerable against the perceived host attack. A smart IDS uncovers hidden attacks, blocking underlying intrusion into systems (Khraisat et al., 2019).

There are four main broad classes or kinds of cyber-attacks: Denial-of-Service (DoS), Remote-to-Local attacks, User-to-Root Attacks, and probing attacks. The first category is Denial-of-Service attacks, which intend to restrict or block services transmitted by the computer or network to different users. In contrast, Remote-to-Local attacks allow cybercriminals to send packets to the user's computer (Khraisat et al., 2019). The aim of probing attacks is to acquire confidential information regarding the computer system or network. When cybercriminals with user-level access acquire admin or root-user access on a certain system or computer, they perform User-to-Root attacks.

A literature review has revealed that cybercriminals utilise various techniques to prevent IDS from detecting and filtering their malicious activities. Cybercriminals' most popular IDS evasion strategies include obfuscation, fragmentation, encryption, and flooding (Khraisat et al., 2019). Cybercriminals use these methods to prevent intrusion detection systems from detecting malicious activities. The current intrusion detection systems experience challenges and cannot detect malicious software when these computer attacks are performed. The most popular IDS evasion strategies are discussed below:

Encryption
Authors of malicious software utilise the security services provided by encryption, including privacy, confidentiality, and integrity, to prevent IDS from identifying their activities and hide attacks targeting specific computer or network systems (Khraisat et al., 2019). The existing intrusion detection systems cannot read or detect encrypted attacks because they cannot match the database signatures with the encrypted content. Encrypted content makes it hard for IDS to recognise malicious software, making it easy for malware authors to steal critical organisational information (Ning et al., 2018). This problem can be solved by implementing smart intrusion detection systems in file server systems to distinguish malware from non-malicious traffic.

Fragmentation
Generally, a packet comprises several smaller packets referred to as fragmented packets. The Internet Protocol (IP) layer includes a recipient node whose function is to reassemble these small packets before transmitting them to the application layer (Khraisat et al., 2019). The network detector must assemble the small packets, and the new packet must be like before fragmentation. Therefore, the intrusion detection system has a data memory that stores fragmented packets to check whether they are like existing database signatures. However, cybercriminals have created new methods, such as fragmentation timeouts and overlap, to conceal attacks and prevent IDS from detecting them (Khraisat et al., 2019). A fragmentation attack allows malware authors to create a malware or malicious packet to change some of the data in the fragmented packets.

Obfuscation
Past research has shown that attackers use obfuscation to ensure IDS does not identify their malware. Hackers use obfuscation to generate messages or information that is hard to comprehend to confuse the IDS. Attackers write the program code in a way that makes it hard to interpret and obscure and cannot be easily detected by reverse engineering processes or static analysis (Khraisat et al., 2019). The existing IDS have limited capabilities to detect this type of attack. Therefore, a smart IDS is needed to address the challenges of the current intrusion detection systems.

Flooding
This kind of cyber-attack intends to make the control mechanism of IDS malfunction by overwhelming the intrusion detection system. IDS allows all traffic when the detector malfunctions (York, 2010). Cybercriminals send large amounts of data at a certain service to confuse or exhaust all detector resources, making it hard for an IDS to identify malware. The massive data amounts

are also sent to create network congestion to prevent legitimate data packets from reaching the destination. This problem can be addressed by implementing smart intrusion detection systems (York, 2010).

Discussion

Malware authors have devised new social engineering and advanced mechanisms to create malicious software that IDS cannot identify. Currently, cybercriminals utilise a sophisticated infrastructure that is difficult to detect and can conceal their conversation and hide their real identities (Khraisat et al., 2019). Thus, smart IDS should be implemented in file server systems to protect computer and network systems because they can detect modern cyber-attack forms, including flooding, obfuscation, etc. Developers of smart IDS should be aware of the limitations and strengths of new research on intrusion detection systems.

Host-based IDS and network-based are the two primary categories of IDSs (Elrawy, Awad & Hamed, 2018). A host-based intrusion detection system is a category of IDS that logs potentially harmful activities, examines traffic, and monitors its installation infrastructure. It is used to shield a specific endpoint from both external and internal attacks. This IDS type can examine a system's logs, monitor running processes, and observe incoming and outgoing traffic. Even though a host-based IDS can monitor the internals of its host computer, its functionality is limited to the host computer. Network traffic is monitored using network-based IDSs. However, a network-based IDS cannot be utilised to monitor devices or computers because they are only limited to monitoring networks (Al-Maksousy, Weigle & Wang, 2018). All data transmitted via the network is checked by NIDS (network-based IDS). Since NIDS makes decisions depending on packet contents and metadata, they can identify different types of attacks. However, NIDS cannot be used to monitor the internal components of the network systems that they safeguard. Therefore, smart IDS should combine these two categories to detect malware effectively.

Smart IDS should be implemented because the existing systems are inaccurate, produce false alerts, and cannot update or generate information regarding contemporary intrusions. A smart IDS is a useful tool that can be implemented by organisations and individuals to shield and detect malware that threatens the availability, confidentiality, and integrity of network and computer systems (Elrawy et al., 2018). It evaluates multiple intercepted network packets and system logs to determine pattern events stored in identified attack databases, including system vulnerabilities. The IDS then tries to take the necessary measures, such as restoring communication channels and alerting emergency teams for action. The primary function of smart IDS is to identify security threats and manage computer and network systems by assessing and keeping computer, information, and network systems under surveillance.

The IDS protects networks and identifies vulnerabilities in three phases. In the first phase, an IDS depends on host-based or network-based sensors to monitor traffic; hence, it is called the monitoring phase. The second phase focuses on identifying patterns and extracting features; thus, it is called the analysis phase. The last phase is called the detection phase, which focuses on identifying misuse or anomaly intrusion. Intrusion detection systems consist of several algorithms to detect potentially harmful malware and threats, analyse all data packets in an information system and monitor all data traffic to identify malware and threats (Elrawy et al., 2018).

One of the benefits of smart IDS is that it intercepts all system alerts generated by traditional intrusion detection mechanisms and performs further investigation to determine whether or not these alerts were generated incorrectly, that is, whether the system is vulnerable to the observed attack (Bhaiji, 2008). IDS also examines user behaviour, operational errors and common mistakes made by regular organisation system users. Smart IDSs can be used to identify network-based attacks and cybercriminals. They offer an extra protection layer and centralised management to allow the system to compare distributed threats and attacks.

Smart IDS includes a web filtering service that offers URL filtering to block access to dangerous, harmful, and inappropriate sites, which may have pharming/phishing attacks, malware like objectionable content or spyware that can expose corporations to legal liability (Kaeo, 1999). Based on targeted research evaluation and automatic research tools, real-time updates allow individuals to implement highly granular rules that filter web access depending on more than seventy-five web content types and more rated sites - all continuously updated through the IDS Network. As a continuous measure, the following will enhance and ensure the maintenance process for any operational IDS system: continuous user involvement and training, regular securing of equipment rooms, continuous improvement on authentication measures and policies, investments in advanced encryption mechanisms, and continuous improvement in daily network audits (Clarke, 1999).

Conclusions

Cyber-attacks and vulnerabilities continue to become more sophisticated due to the rapid technology growth. The existing IDS experience several challenges and cannot detect particular attacks because cybercriminals use sophisticated methods to hide their attacks or malware. Intrusion detection systems are the next-generation protection that provides the visibility to identify advanced legitimate threats within content, even from authorised applications and trusted sources. This protection allows novel applications into the network but automatically blocks any potentially harmful activity or behaviour. IDS detailed security knowledge provides rapid service/product updates and offers protection from emerging and new threats.

A smart intrusion detection system offers Fortinet clients the latest defences against stealthy network-level threats. It utilises a customisable database of more than any known threats to allow appliances to identify and block attacks that evade conventional firewall defences. It also offers behaviour-based heuristics, allowing the system to identify threats for which no signature has yet been created. The combination of unknown and known threat prevention allows the systems to block the most harmful threats at the network border, regardless of whether the network is wireless or wired or at the corporate branch office or corporate headquarters. Smart intrusion detection systems also include a web filtering service that offers URL filtering to stop access to dangerous, harmful and inappropriate sites that may consist of pharming/phishing attacks, malware like objectionable content or spyware, which can expose corporations to legal liability.

When implementing smart intrusion detection systems, information technology (IT) professionals should place the IDS on a demilitarised zone or a screened subnet to ensure that an organisation's local area network remains secure, and the corporation can access untrusted networks without fear of cyber-attackers. Smart IDSs should be implemented in front of file server systems and behind the firewall to ensure all malware is filtered. They should be properly installed to ensure that it notifies users when malicious software is sent to their computer or network systems. A successful information security program requires adequate support from senior management. Therefore, implementing smart IDSs requires support from senior management for the process to be successful. Regular updates and maintenance are also important to ensure the intrusion detection system functions effectively and efficiently.

References

Al-Maksousy, H. H., Weigle, M. C., & Wang, C. (2018). NIDS: Neural network-based intrusion detection system. In 2018 IEEE International Symposium on Technologies for Homeland Security (HST), 1-6.

Aspers, P., & Corte, U. (2019). What is qualitative in qualitative research? *Qualitative Sociology, 42*, 139-160.

Bhaiji, Yusuf (2008). *Network Security Technologies and Solutions (CCIE Professional Development Series).* Cisco Press.

Canavan, J. E. (2001). Fundamentals of Network Security, Artech House Publishers. 1st edition proceeding of the 7th Australian Information Security Management

Conference.

Clarke, R. (1999). Introduction to data protection and data protection and definitions of terms. In 1999 IEEE 2nd international conference on cyber security and cloud computing, 307-311.

Elrawy, M. F., Awad, A. I., & Hamed, H. F. (2018). Intrusion detection systems for IoT-based smart environments: a survey. *Journal of Cloud Computing, 7*(1), 1-20.

Jabez, J., & Muthukumar, B. (2015). Intrusion detection system (IDS): anomaly detection using outlier detection approach. *Procedia Computer Science, 48*, 338-346.

Kaeo, M. (1999). *Designing Network Security.* Cisco Press.

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity, 2(1)*, 1-22.

Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications, 36(1)*, 16-24.

Nichols, R. Ryan, D., & Ryan, J. (2000). Defending your Digital Assets against Hackers, Crackers, Spies and Thieves, RSA Press.

Ning, J., Xu, J., Liang, K., Zhang, F., & Chang, E. C. (2018). Passive attacks against searchable encryption. *IEEE Transactions on Information Forensics and Security, 14(3)*, 789-802.

York, D. (2010). *Seven deadliest unified communications attacks*. Syngress.