COS30015 IT Security
Research Project

Topic: Intrusion Detection System

Name: Phang Xia Hui
Student ID: 1027773508
Tutorial Group: Thursday
Submission Date / Time: 15 October 2023,
Week 6, Sunday, 10:10 pm.
Due Date / Time: 15 October 2023,
Week 6, Sunday, 11:59 pm.

Abstract

With the growing integration of the digital realm into our everyday activities, the significance of cybersecurity cannot be emphasized enough. This literature study explores the significance of Intrusion Detection Systems (IDS) in the current period dominated by communication technologies, the Internet, and emerging concepts such as the Internet of Things (IoT) and 5G networks. Moreover, this study laid a solid groundwork by commencing with an analysis of the core issue and fundamental concepts. This comprehensive literature review provides a detailed examination of the existing systems and methodology along with an evaluation of the primary concerns and challenges in the field. The review encompasses a comprehensive analysis of a specific example or case, including a study of both positive and negative arguments, personal ideas, and clear-cut results lastly ending with conclusion of the report.

1. Introduction

1.1 Definitions of the Problem and Key Terms

The 2017 Symantec Internet Security Threat Report (Symantec 2017) states that there were more than three billion zero-day assaults in 2016. Cyberattacks are becoming more complex, making breach detection harder. Secure data confidentiality, integrity, and availability may lose trust if incursions continue (Khraisat et al. 2019). Ashoor and Gore (2011) suggested firewalls and encryption to prevent unauthorised access and protect computer infrastructure. Despite these precautions, the intruders broke into the computers. Computer intruders, publicly available online, constitute a major threat to society (Ashoor & Gore 2011). Additionally, Kashyap et al. described a firewall as a hardware or software barrier between computer networks. It separates networks and enforces specific restrictions to prevent assaults (2013). The fact that firewalls only block external assaults but not internal ones shows that they are insufficient (Kashyap et al. 2019). These scenarios provide intrusion detection systems (IDS) control. IDSs stop attacks, reduce recovery losses, and identify security issues to avoid future attacks (Kashyap et al. 2013). Intrusion Detection Systems (IDS) monitor computers and networks for attacks and other system misuse (Kashyap et al. 2013).

1.2 Adequate Background

Intrusion detection systems (IDSs) are sophisticated software or hardware systems that are specifically engineered to observe and scrutinize events taking place on a computer system or network with the purpose of detecting possible security risks (Bace & Mell 2001, p. 5). In recent years, the frequency and intensity of network attacks have increased, leading to the growing importance of intrusion detection systems in the security infrastructure of most organisations (Bace & Mell 2001, p. 5).

Implementing robust security measures is crucial to safeguard a system from unauthorised intrusion and protect its data and resources (Sundaram 1996). However, it is currently impractical to entirely prevent security flaws. Nevertheless, we can strive to identify these infiltration attempts in order to afterwards implement measures to mitigate the harm. The subject is commonly known as intrusion detection (Sundaram 1996). Anderson introduced the notion of intrusion detection in 1980, as cited by Sundaram in 1996. Sundaram (1996) provides a clear definition of an intrusion attempt as a purposeful and unauthorised endeavour to obtain access to information, manipulate information, or undermine the dependability or usability of a system. Intrusion detection involves the continuous monitoring of computer systems or networks to identify any attempts to compromise the system or network's confidentiality, integrity, or availability (Bace & Mell 2001, p. 5). Intrusions encompass various scenarios, such as malevolent individuals exploiting the Internet to unlawfully infiltrate

systems, authorized users attempting to acquire privileges above their authorized level, and authorized users abusing the privileges bestowed upon them (Bace & Mell 2001, p. 5). Intrusion detection systems (IDSs) optimize the process of monitoring and analysing tasks. Intrusion Detection Systems (IDSs) can be implemented as either software or hardware (Bace & Mell 2001, p. 5).

1.3 Convincible Importance

Based on the Data Breach Statistics for 2017, it has been reported that hackers have compromised or taken nearly nine billion data records since 2013 (Kashyap et al. 2019). According to a Symantec report, there is a rising trend in the frequency of security breach incidences. Historically, criminals mostly focused on defrauding individuals who held accounts with financial institutions, by unlawfully acquiring their credit card information or gaining unauthorized access to their bank accounts (Kashyap et al. 2019). Notable instances of cybercrime have demonstrated the rapid global dissemination of threats and the potential for even a minor breach to significantly impact a company's critical operations. Globally, there exists a substantial number of cybercriminals who are motivated to illicitly acquire information, generate unlawful profits, and actively pursue new targets (Kashyap et al. 2019).

Currently, intrusion detection systems are being imported worldwide due to their ability to protect enterprises' infrastructure from hazards arising from increased network connectivity and dependence on information systems (Bace & Mell 2001, p. 5). The quandary faced by security experts is not whether to employ intrusion detection, but rather which specific characteristics and capabilities of intrusion detection to implement, taking into consideration the scale and nature of modern network security threats (Bace & Mell 2001, p. 5).

Despite the implementation of many techniques, such as firewalls and encryption, to safeguard network infrastructure from unauthorized access through the Internet, security remains a significant issue for business and institutional networks (Ashoor & Gore 2011). Each invasion has the objective of surreptitiously accessing the data networks of these companies and web services (Ashoor & Gore 2011). IDS is a comparatively novel technique in comparison to other recently established intrusion detection systems (Ashoor & Gore 2011). An intrusion detection system in a network serves as a means to aid computer systems in predicting and reacting to network invasions (Ashoor & Gore 2011). In addition to that, intrusion detection functions encompass monitoring and analysing system and user activity, evaluating system settings and vulnerabilities, assessing system and file integrity, identifying attack-specific patterns, detecting user policy violations, and analysing abnormal activity patterns (Ashoor & Gore 2011).

Bace and Mell (2001, p. 5) state that intrusion detection systems have the ability to reduce problem behaviours by heightening the perceived likelihood of being detected and punished for those who abuse the system. When conventional security measures prove ineffective in preventing an attack or security breach, the purpose of documenting the threat to an organization is to serve as a quality control mechanism for security design and administration, particularly in the context of large and intricate enterprises. Additionally, it aims to provide valuable information about actual intrusions in order to enhance the process of diagnosing, recovering from, and rectifying the underlying causes. These tasks also involve detecting and responding with attack preambles (such as network probes and other "doorknob rattling"), recognizing an organization's threat, and documenting it (Bace & Mell 2011, p. 6). IDS collects data from computer systems and networks to help them fight threats (Ashoor &

Gore 2011). It then compares this data to discriminatory patterns to identify attacks or weaknesses (Ashoor & Gore 2011).

2. Literature Review

2.1 Major Issues or Challenges

Intrusion detection systems are still in their infancy today and require further research to become even more effective. The current intrusion detection system has a vast array of problems and difficulties that require immediate and intense research attention (Beigh, Bashir & Chahcoo 2013). Despite much research on IDSs, several crucial issues still need to be resolved. Recently, false alarm rates and detection accuracy have emerged as the key concerns and problems in creating effective IDS (Sabri, Norwawi & Seman 2011). In order to effectively identify various intrusions and reduce the occurrence of false alarms, Intrusion Detection Systems (IDSs) must demonstrate improved precision. Additionally, they should possess the ability to overcome various problems encountered in their operation (Beigh, Bashir & Chahcoo, 2013).

2.1.1 False Alarm Rate

A false positive, often referred to as a false alarm, is an alert that is activated by normal, non-malicious background traffic (Mell et al. 2003). Measuring false alarms can be hard because to the absence of a universally applicable network standard and the variable false positive rate of an IDS, which depends on the network environment (Mell et al. 2003). Moreover, it is difficult to discern characteristics of network traffic or host behaviour that will lead to inaccurate alerts. Thus, it can be difficult to guarantee the replication of the same quantity and diversity of false alarms in an Intrusion Detection System (IDS) test as those found in real networks (Mell et al. 2003).

2.1.2 Detection Policy

Furthermore, the detection policy poses additional difficulties when it comes to constructing intrusion detection systems. The detection strategy is the primary determinant in distinguishing between a malicious attack and helpful information necessary for the user to do a task or job (Beigh, Bashir & Chahcoo 2013). The detection algorithm should possess sufficient capability to rapidly match every case, while also effectively matching the terms. The detection policy can be categorised as either misuse-based or anomaly-based. Anomaly-based detection involves identifying patterns of behaviour and classifying them as attacks if they deviate from the expected norm (Beigh, Bashir & Chahcoo 2013). In an alternative situation, the pattern is evaluated using a pattern matching algorithm designed to detect known attacks. If the pattern completely matches with any questionable data, it is categorised as an attack. Nevertheless, there are constraints in the system as it lacks guidelines for identifying new attacks. Consequently, these new attacks may go undetected or only be recognised if they modify the data in a manner that prohibits them from conforming to the established pattern. In order to effectively counter the majority of attacks, it is necessary to have a robust and efficient algorithm that can accurately and swiftly identify the pattern (Beigh, Bashir & Chahcoo 2013).

2.1.3 Deficiency or incomplete Data set

The dataset comprises all survey data that will undergo analysis. The efficacy of an intrusion detection system hinges on the calibre of the datasets employed. Therefore, the near-real-time datasets were crucial (Beigh, Bashir & Chahcoo 2013). Scientists are now utilizing outdated data sets such as DARPA 98, 99, recent Mexico university immune system, etc. However, due to their age, we are unable to effectively counteract the relatively recent risks they represent (Beigh, Bashir & Chahcoo 2013). Consequently, it became imperative to assess

attack models using current data sets. Hence, to attain the utmost accuracy and clarity, it is imperative to address this matter (Beigh, Bashir & Chahcoo, 2013).

2.1.4 Testing and evaluation of IDS

Intrusion Detection Systems (IDS) have gained widespread acceptance as a standard method for assuring the security of large networks, and the amount of data being processed is growing rapidly. Despite the significant financial investments made by companies in IDS technology, there is currently a lack of proven scientific methods to assess its effectiveness (Beigh, Bashir & Chahcoo 2013). Although multiple quantitative methods have been devised to assess effectiveness, they do not assign effectiveness ratings on a uniform scale. These approaches consider several variables such as coverage, risk of false alarms, risk of detection, resilience against assaults on intrusion detection systems, bandwidth and traffic processing capabilities, and capacity for detecting attacks (Beigh, Bashir & Chahcoo 2013). Hence, they are inadequate for assessing the efficacy of the IDS. Furthermore, there should be a universally accepted scale for evaluating or quantifying the effectiveness of Intrusion Detection Systems (IDS). The diverse issues encompass the collection of victim software and scripts, experimentation with different settings, and the diverse requirements for IDS testing (Beigh, Bashir & Chahcoo 2013).

2.2 Major Systems

The three primary types of intrusion detection systems are Network Intrusion Detection Systems (NIDS), Host Intrusion Detection Systems (HIDS), and hybrid intrusion detection systems.

2.2.1 Network Intrusion Detection System (NIDS)

Network system managers need NIDSs to discover security gaps in a company's network (Javaid et al. 2016). Network system managers need NIDSs to discover security gaps in a company's network (Javaid et al. 2016). NIDSs monitor and analyse network traffic entering and leaving a company's network devices. If an unauthorized entry is discovered, audible alarms are activated. The classification of NIDSs is determined by intrusion detection technologies, which can be categorized into two types: signature-based (SNIDS) and anomaly detection-based (ADNIDS). SNIDS and NIDS have installed attack signatures. Pattern matching is a method that compares network traffic with predefined signatures in order to identify instances of network intrusions (Javaid et al. 2016). Nevertheless, ADNIDS identifies network traffic as an intrusion when it diverges from the established norm (Javaid et al. 2016). Javaid et al. (2016) proved that the SNIDS system effectively and accurately detects known threats with a high level of precision and a minimal amount of false alarms. Because an IDS can only store so many attack signatures, it performs poorly at identifying unknown or innovative attacks (Javaid et al. 2016). However, ADNIDS excels at detecting new threats. Due to its capacity to identify novel assaults, ADNIDS is routinely used by researchers despite its high false-positive rates (Javaid et al. 2016).

2.2.2 Host-Based Intrusion Detection System (HIDS)

A Host-Based Intrusion Detection System (IDS) is a security tool that observes and logs the actions of a single computer or network host, with the purpose of identifying any suspicious or harmful behaviour (Jose et al. 2018). HIDS primarily monitors process activity and protects the security of system data, system logs, and registry keys. Anomaly detection techniques are beneficial in intrusion detection systems because they can distinguish between the routine operation of a system and any intrusive behaviour. Host-based intrusion detection systems are

deployed on particular systems and employ methodologies to gather and analyse data related to those specific systems (Jose et al. 2018). Host-based Intrusion Detection Systems (HIDS) can be used to identify inefficient consumption of corporate resources. In order to thwart the assault, it is recommended to cease the utilization of company resources if it exhibits a comparable pattern to prior attacks (Jose et al. 2018). Host-based intrusion detection systems oversee, detect, and react to user system actions and host threats (Jose et al. 2018).

2.2.3 Hybrid Intrusion Detection System

To tackle the shortcomings of existing intrusion detection systems, such as their frequent generation of false-positive alarms and limited ability to detect new threats, researchers have developed hybrid intelligent systems (Maseno et al. 2022). The hybrid technique integrates both misuse-based and anomaly-based approaches. The hybrid technique effectively addresses the limitations of the two legacy IDSs. Research findings indicate that hybrid detection systems exhibit superior performance compared to single intrusion detection systems (Maseno et al. 2022).

2.3 Major Method

2.3.1 Signature-based intrusion detection systems (SIDS)

Signature-based intrusion detection systems (SIDS), often referred to as Knowledge-based Detection or Misuse Detection, utilize pattern matching algorithms to identify recognized threats (Khraisat et al. 2019). Intrusion detection systems (IDS) utilize matching techniques to identify a previous unauthorized access. Essentially, an alarm signal is activated when a detection pattern corresponds to one that already exists in the database for a prior incursion (Modi et al. 2013). In the context of Signature-based Intrusion Detection Systems (SIDS), the analysis of the host's logs is conducted to discover patterns of commands or actions that have been previously recognized as potentially harmful malware. Generally, SIDS demonstrates a high level of precision in identifying recognized intrusions (Kreibich & Crowcroft 2004). Nevertheless, Intrusion Detection Systems (IDS) face challenges when it comes to detecting zero-day attacks due to the absence of a pre-existing signature in the database until the signature of the new assault is acquired and saved. SIDS are utilized in various well-known software applications, including Snort and NetSTAT (Roesch 1999).

2.3.2 Anomaly-based intrusion detection system (AIDS)

Machine learning, statistical analysis, and knowledge-based methods are used to build AIDS computer system behaviour models (Butun, Morgera & Sankar 2013). When observed behaviour differs significantly from the model, anomalies are incursions. This category of strategies assumes harmful behaviour differs from normal user behaviour. User behaviour that deviates from expectations is called an intrusion (Butun, Morgera & Sankar 2013). AIDS development involves two phases: training and testing. The typical traffic profile is used to develop a normal behaviour model. A new data set is used to test the system's ability to generalize to undiscovered incursions. Statistical, knowledge-based, or machine learning training can classify AIDS (Butun, Morgera & Sankar 2013). Alazab et al. (2013) stated that the AIDS system can detect zero-day assaults without a signature database. AIDS warns of unusual behaviour. AIDS has other benefits. Internal trauma is first identified. Intruders using a stolen account make unusual transactions, setting off the alarm. Cybercriminals struggle to recognize habitual user behaviour without suspicion due to tailored profiles (Khraisat et al. 2019).

3. Case Study in Haystack: An Intrusion Detection System

Smaha's 1988 case study explores the implementation of an intrusion detection system called "Haystack". The Haystack system was created as a prototype to identify breaches in Air Force computer systems that are used by multiple users. The Haystack system aimed to condense extensive system audit trails into concise summaries of user behaviours, abnormal occurrences, and security breaches, facilitating the detection and examination of intrusions by System Security Officers (SSOs), with a special focus on authorized users (Smaha 1988).

Haystack was developed in response to many initiatives in the field of computer security. The procedures included the development of multi-vendor operating system standards like POSIX, the creation of legislative laws for computer security, and the necessity to follow standards when purchasing computer systems (Smaha, 1988). The National Computer Security Centre (NCSC) Trusted Computer System Evaluation Criteria, commonly referred to as DOD 5200.28-STD, had a crucial impact on establishing benchmarks for assessing the security of computer systems (Smaha 1988). POSIX played a crucial role in standardising operating system interfaces. The recognition that a substantial number of computer crimes were committed by individuals within the organisation, including trustworthy employees, led to the need for improved intrusion detection systems (Smaha 1988).

The Haystack case study displays key intrusion detection system features. Managing multi-user systems' massive audit trail data requires real-time processing (Smaha 1988). In addition, the study emphasises that there are various intrusion categories and that recognising them requires multiple methods. Intrusion detection systems are tough to build due to the situation's complexity (Smaha 1988). The paper proposes combining individual and group user models and acknowledges the difficulty of describing them. Modifying models to reflect user behaviour changes is another issue (Smaha 1988).

Moreover, this paper examines the notable advantages of Haystack’s intrusion detection system. Firstly, it efficiently reduces data overhead by condensing vast audit records into brief, significant security events. The decrease in data volume streamlines the responsibilities of System Security Officers (SSOs), preventing them from being inundated with unprocessed, unmanageable records. Instead, they are presented with a concise and controllable summary of potential security issues (Smaha 1988). Secondly, Haystack’s incorporation of both individual and group user models allows for a more accurate depiction of typical user actions, hence improving the system’s capacity to identify abnormalities and potential breaches (Smaha 1988). Furthermore, the ability to analyse user activity trends over time allows for a proactive approach in spotting emerging dangers and detecting efforts by malevolent insiders to manipulate the system, thereby strengthening the system’s security defences (Smaha 1988). To summarize, Haystack’s method integrates efficient data management, precise user behaviour analysis, and proactive threat identification, resulting in a strong intrusion detection system.

While the Haystack intrusion detection system offers advantageous characteristics, it also presents substantial challenges. A crucial limitation is the event horizon constraint, mostly dictated by processing capacity. When confronted with practical scenarios, particularly on larger systems, it might be challenging to comprehensively examine all user sessions promptly, perhaps leading to some activity being overlooked (Smaha 1988). Another notable constraint is the absence of a consensus over the specific attributes of security rules. The system's ability to efficiently identify intrusions may be compromised due to the absence of uniform and clearly defined concept of "bad behaviour" caused by inconsistent security standards and

interpretations (Smaha 1988). Attaining the delicate balance between reducing data overhead and minimising both false positives (incorrectly recognising non-intrusive activities as suspicious) and false negatives (failing to detect actual intrusions) poses an extra significant challenge (Smaha 1988). In summary, Haystack has valuable intrusion detection capabilities, however it encounters difficulties concerning event horizon constraints, policy inconsistencies, and the need for precise threshold management to minimise erroneous warnings.

4. Personal views and ideas

In my view, Haystack's approach to intrusion detection represents a substantial advancement in addressing the urgent problem of insider threats. It is critical to have a system that can accurately identify user behaviour anomalies since, as the case study rightly points out, the bulk of security breaches are carried out by authorized users. A novel method of intrusion detection uses the combination of individual and group user models to provide a thorough understanding of what defines typical activity.

Nevertheless, the constraint imposed by the event horizon is a valid concern, particularly when dealing with large and intricate systems. In the realm of cybersecurity, time is of utmost importance, and any delay in detecting potential attacks can have disastrous consequences. In order to provide effective real-time monitoring of user behaviour, it is crucial to determine methods for expanding the event horizon.

Furthermore, companies must acknowledge the absence of consensus around security rules. Although the existence of universally acknowledged security standards would be desirable, their practical implementation would pose significant challenges. Consequently, intrusion detection systems must possess the ability to adjust and be flexible in order to accommodate various security needs. Security experts must consistently improve their systems to achieve an optimal equilibrium between reducing the occurrence of false positives and false negatives.

The novel methodology employed by Haystack to detect unauthorized access presents a possible answer to the escalating issue of internal security vulnerabilities. Nevertheless, it is essential to enhance the capacity to surpass the constraints of the event horizon and enhance flexibility to comply with unique security regulations, hence guaranteeing its efficacy in diverse organizational contexts. The field of cybersecurity is continuously changing, requiring intrusion detection systems to adapt and innovate in order to stay ahead of new threats and preserve a competitive advantage.

5. Conclusion

This research review highlights the critical importance of intrusion detection systems (IDS) in the dynamic digital environment as a whole. An intrusion detection system (IDS), which strengthens conventional security measures, is essential in cybersecurity due to the rising frequency of zero-day assaults and complex cyber threats. The analysis has highlighted several impediments, including incorrect warnings, detection processes, datasets, and evaluation approaches, that necessitate ongoing inquiry to enhance the precision of Intrusion Detection Systems (IDS). The paper analyses various categories of Intrusion Detection Systems (IDS), such as Network Intrusion Detection Systems (NIDS), Host Intrusion Detection Systems (HIDS), and hybrid systems, tailored to address specific security requirements. The case study of Haystack's intrusion detection system showcased the efficacy of data management and user behaviour analysis, while also highlighting concerns around the constraints of event horizon and discrepancies in policy. It is crucial to modify Intrusion Detection Systems (IDS) in order

to meet changing security requirements and address emerging risks. Amidst the ever-changing cybersecurity environment, Intrusion Detection Systems (IDS) continue to be a fundamental element in safeguarding digital assets.

List of References:

Alazab, A, Abawajy, J, Hobbs, M, Layton, R & Kraisat, A 2013, 'Crime toolkits: the productisation of cybercrime', 2013 12th IEEE international conference on trust, security and privacy in computing and communications, pp. 1626-1632, viewed 13 October 2023, < https://doi.org/10.1109/TrustCom.2013.273>

Ashoor, AS & Gore, S 2011, 'Importance of intursion detection system (IDS)', International Journal of Scientific and Engineering Research, vol. 2, no. 1, pp. 1-4, viewed 3 October 2023, < https://portal.arid.my/Publications/f3da7cd3-5bab-4294-94d1-6a22c1d4235d.pdf>.

Bace, RG & Mell, P 2001, 'Intrusion detection systems', UCCS, viewed 23 September, < http://cs.uccs.edu/~cchow/pub/ids/NISTsp800-31.pdf>.

Beigh, BM, Bashir, U & Chahcoo, M 2013, 'Intrusion detection and prevention system: issues and challenges', International Journal of Computer Applications, vol. 76, no. 17, viewed 22 September 2023, < https://www.researchgate.net/profile/Nirmala-Svsg/post/What_are_the_challenges_of_Intrusion_Detection_Systems_IDS/attachment/59d6402779197b807799c685/AS%3A429770749026308%401479476739326/download/Intrusion+Detection+and+Prevention+System+-++Issues.pdf>.

Butun, I, Morgera, SD & Sankar, R 2013, 'A survey of intrusion detection systems in wirelesss sensor networks', IEEE communications surveys & tutorials, vol. 16, no. 1, pp. 266-282, viewed 4 October 2023, < https://doi.org/10.1109/SURV.2013.050113.00191>.

Javaid, A, Niyaz, Q, Sun, W & Alam, M 2016, 'A deep learning approach for network intrusion detection system', In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), pp. 21-26, viewed 2 October 2023, < https://dl.acm.org/doi/pdf/10.4108/eai.3-12-2015.2262516>.

Jose, S, Malathi, D, Reddy, B & Jayaseeli, D 2018, 'A survey on anomaly based host intrusion detection system', Journal of Physics: Conference Series, vol. 1000, p. 012049, viewed 7 October 2023, < https://iopscience.iop.org/article/10.1088/1742-6596/1000/1/012049/pdf>.

Kashyap, S, Agrawal, P, Pandey, VC & Keshri, SP 2013, 'Importance of intrusion detection system with its different approaches', International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 2, no. 5, pp. 1902-1908, viewed 23 September 2023, < http://www.ijareeie.com/upload/may/24_Importance.pdf>.

Khraisat, A, Gondal, I, Vamplew, P & Kamruzzaman, J 2019, 'Survey of intrusion detection systems: techniques, datasets and challenges', Cybersecurity, vol. 2, no. 1, pp. 1-22, viewed 21 September 2023, < https://doi.org/10.1186/s42400-019-0038-7>.

Kreibich, C & Crowcroft, J 2004, 'Honeycomb: creating intrusion detection signatures using honeyspots', ACM SIGCOMM computer communication review, vol. 34, no. 1, pp. 51-56, viewed 11 October 2023, < https://dl.acm.org/doi/pdf/10.1145/972374.972384?casa_token=6B6CT-7fE38AAAAA:2An7Kqz9rZKoSTqWIG4cUYhICFzepQhl9scazYRrp0iJICJtqNAEVFL_peuUzWqTCEQ-wdJX5JjcxQ> .

Maseno, EM, Wang, Z & Xing, H 2022, 'A systematic review on hybrid intrusion detection system', Security and Communication Networks 2022, viewed 9 October 2023, < https://downloads.hindawi.com/journals/scn/2022/9663052.pdf?_gl=1*1brihz9*_ga*MTgxNTI5MjYzNy4xNjk3Mjg5MTU4*_ga_NF5QFMJT5V*MTY5NzQyNjAxMC4zLjEuMTY5NzQyNjY3Ni42MC4wLjA.&_ga=2.169843362.2032981723.1697289158-1815292637.1697289158>.

Mell, P, Hu, V, Lippmann, R, Haines, J & Zissman, M 2003, 'An overview of issues in testing intrusion detection systems', viewed 1 October 2023, < https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50745>.

Modi, C, Patel, D, Borisaniya, B, Patel, H & Rajarajan, M 2013, 'A survey of intrusion detection techniques in cloud', Journal of network and computer applications, vol. 36, no. 1, pp. 42-57, viewed 10 October 2023, < https://www.sciencedirect.com/science/article/pii/S1084804512001178/pdfft?casa_token=JmRlzGo9xR0AAAAA:Hfkugpnst2h-f72e0oeyJLKZUPHKVFaLGcI2tT9Q7fuPAxvdLaJKuZ_2-id5SqQ8WorPuGj1cMc&md5=ce399a943650265d3bfe9b525c573737&pid=1-s2.0-S1084804512001178-main.pdf>.

Roesch, M 1999, 'Snort: Lightweight intrusion detection for networks', Lisa, vol. 99, no. 1, pp. 229-238, viewed 8 October 2023, < https://www.usenix.org/legacy/publications/library/proceedings/lisa99/full_papers/roesch/roesch.pdf>.

Sabri, FN, Norwawi, NM & Seman, K 2011, 'Identifying false alarm rates for intrusion detection system with data mining', IJCSNS: International Journal of Computer Science and Network Security, vol. 11, no. 4, pp. 95-99, viewed 30 September 2023 < https://d1wqtxts1xzle7.cloudfront.net/30259108/20110414-libre.pdf?1390882236=&response-content-disposition=inline%3B+filename%3DIdentifying_False_Alarm_Rates_for_Intrus.pdf&Expires=1697233516&Signature=VfPZnBOARL~1-pWPDMbmDj4FjABevieKVpP5sEbqaMvo4bVw13pRMJV3GDpGykHlQcy0pOE3l9gLR2BdqAQxXOZ4B76NiIncXTp2x0lDuwJfvX2~GjOOMx6L6l2WhAci1I1U-y1Kr29C6RoDeoAyJxMpZX67swgP8ikgOUZqT5sSMFKX66iSBd1FB5D2qLHM0FlxLVN7LjocfOudJR~qdUeOjoZ-5a9hDH5G1yq01~or0aSAvhuFEoHfi00e7ZbarUZvfV-wa72eMDNAID0Ald2KgIHTj-ETyzXn3VS4~cl6Vg4zQu7ame79WHIw8~8eNh4MMhH7ymHgAK5pFPTLNw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA>.

Smaha, SE 1988, 'Haystack: An intrusion detection system' Fourth Aerospace Computer Security Applications Conference, vol. 44, p. 37, viewed 7 October 2023, < https://homeostasis.scs.carleton.ca/~soma/id-2007w/readings/smaha-haystack.pdf>.

Sundaram, A 1996, 'An introduction to intrusion detection', Crossroads, vol. 2, no. 4, pp. 3-7, viewed 24 September, <https://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/D-mining/Anomaly-D/Intrusion-detection/Intrusion-Detection-Intro.pdf>.

Symantec 2017, 'Internet security threat report 2017', vol. 22, 7010, viewed 21 September 2023, < https://docs.broadcom.com/doc/istr-22-2017-en>.