Indonesian of Health Information Management Journal (INOHIM) ISSN (Print) : 2354-8932
Vol.10, No.1, Juni 2022, p.10-17, DOI: 10.47007/inohim.v10i1.396 ISSN (Online) : 2655-9129

SIMRS Network Security Simulation Using Snort IDS and IPS Methods

Wahyu Wijaya Widiyanto
Politeknik Indonusa Surakarta, Surakarta, Indonesia
Jl. Cemani No.8, Grogol, Sukoharjo, Indonesia
Korespondensi E-mail: wahyuwijaya@poltekindonusa.ac.id

Submitted: 4 Maret 2022, *Revised:* 25 April 2022, *Accepted:* 10 Mei 2022

Abstract

Hospital information systems have an essential role in clinical and administrative services. This triggers an innovation that supports an integrated quality measurement data management system by integrating the Hospital Management Information System (SIMRS). SIMRS can be implemented locally or in the cloud, using the network to exchange data and information. Along with the current development of Information Technology, information security is very important, especially on a network connected to the internet. But what is unfortunate is that developments in the security system itself do not accompany the imbalance between each technological development. This study aims to overview techniques for securing network computers from various attacks through network security simulations. The research method used is using Snort as a detector to perform security on computer networks, while as a system for detecting and preventing intruders on computer network servers using the Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) methods. This study concludes that the IDS system with Snort simulated can detect attacks with the same average accuracy value of 99.97% and produce an average server response time value by good snort rules (1 client is 0.50 seconds, 2 clients are 0.32) seconds.

Keywords: *network security, snort, IDS, IPS*

Abstrak

Sistem informasi rumah sakit memiliki peran penting dalam pelayanan klinis dan administrasi. Hal ini memicu inovasi yang mendukung sistem pengelolaan data pengukuran mutu yang terintegrasi dengan mengintegrasikan Sistem Informasi Manajemen Rumah Sakit (SIMRS). Implementasi SIMRS dapat dilakukan secara lokal maupun cloud, keduanya menggunakan jaringan untuk bertukar data dan informasi. Seiring dengan perkembangan Teknologi Informasi saat ini, keamanan suatu informasi menjadi sangat penting terutama pada suatu jaringan yang terkoneksi dengan internet. Namun yang disayangkan, ketimpangan antara setiap perkembangan teknologi tersebut tidak dibarengi dengan perkembangan sistem keamanan itu sendiri. Penelitian ini bertujuan untuk memberikan gambaran tentang teknik pengamanan jaringan komputer dari berbagai jenis serangan melalui simulasi keamanan jaringan. Metode penelitian yang digunakan adalah menggunakan Snort sebagai pendeteksi untuk melakukan pengamanan pada jaringan komputer, sedangkan sebagai sistem untuk mendeteksi dan mencegah penyusup pada server jaringan komputer menggunakan metode Intrusion Detection Systems (IDS) dan Intrusion Prevention Systems (IPS). Kesimpulan dari penelitian ini adalah sistem IDS dengan simulasi Snort dapat mendeteksi serangan dengan nilai akurasi rata-rata yang sama yaitu 99,97%, dan menghasilkan nilai rata-rata waktu respon server dengan aturan snort yang baik (1 client adalah 0,50 detik, 2 client adalah 0,32) detik.

Kata Kunci*:* keamanan jaringan, snort, IDS, IPS

Introduction

Implementing a Management Information System (MIS) for a hospital is very important in its application in today's era. This matter is supported by the increasingly complex problems in the patient's medical data and other administrative data related to service delivery the hospital accepted by the patient. However, providing SIM service is not easy, especially regarding costs Procurement of SIM is not small. SIM Application requires careful planning. When done in a hurry without going through the planning stage, it is feared that it costs more money and more risky SIM failure occurs (1).

Hospital institutions are constantly under pressure to improve medical services, reduce medical errors, provide timely access to information, and at the same time monitor service activities and control operational costs. To meet these demands, hospitals must have an integrated management information system (MIS) that can share real-time, precise, and accurate information. However, this management

information system cannot run automatically if it is not supported by software or enterprise software systems already embedded in the hospital server. According to the world body WHO, an information system is a system that provides information for the decision-making process at every level within an organization (2). The hospital information system (SIRS) is a system that integrates data collection, processing, reporting, and use of information needed to improve the efficiency and effectiveness of health services through better management at various levels of health services. In contrast, the hospital management information system (SIMRS) is an information system specifically designed to assist the management and planning of health programs (3).

Technological developments, especially in the field of Networking, make a variety of things features, technology, and tools develop naturally fast and good (Acai Sudirman, Muttaqin Muttaqin, Ramen A. Purba, Alexander Wirapraja, Leon A. Abdillah, Fajrillah Fajrillah, Fatimah Nur Arifah, Julyanthry Julyanthry, Ronal Watrianthos, 2020);(5);(6);(7);(8);(9);(10);(11). Computer and network technology provide convenience for the public, especially the internet. This convenience certainly poses a great danger of being vulnerable to threats in using the internet. Many threats and attacks that occur come from the network itself and even from the internet network. This happens because resources, services, and others are public, so a special system is needed to maintain the resources and services on the computer network (12). A computer network must provide a sense of security for access performed by a user by giving an information guarantee, or personal data is safe from access by an intruder. A server's security is difficult to monitor for 24 hours (13).

Computer networks can be weakened or less than optimal when the computer network is attacked by intruders or hackers and crackers for the benefit or benefit of other parties (14); (15). An intruder is a hacker or cracker who always tries to access a security system. This system intrusion occurs when an unauthorized person tries to gain access or interferes with the regular operation of an information system (16). Network security threats such as attackers, intruders, and crackers are increasingly widespread. Therefore, any information on the hospital computer network system must be kept confidential or data privacy so that it is not used by parties who do not have the right to use the information on the server computer (17).

One method for securing resources and services on a computer network is Intrusion Detection Systems (IDS) which function as intruder detection systems. With IDS, suspicious network activities can be immediately identified. At the same time, Intrusion Prevention Systems (IPS) serve as intruder prevention systems, IPS works as a deterrent to intruders who will carry out attacks with Snort (18). Snort is a tool used in Intrusion Prevention Systems (IPS) that functions as an alert to secure computer networks. Computer network systems often have problems increasing network traffic and activity quickly without identifying and detecting the cause. So, we need a system that can protect and provide security for any data traffic on a computer network. Several tools can be used for network monitoring systems that impact computer attacks, one of which is IDS-based Snort (19).

Snort is an IDS-based application that can recognize attack patterns based on created rules. Each attack identified by snort will generate an alert placed in a database for identification purposes by the administrator. This research is limited to the main problem, namely only the configuration of the IDS method with Snort and the IPS method with IPTables or Firewall, Snort server is implemented on the Ubuntu Linux operating system and BASE snort as a web monitoring attack. The test is carried out simply as a simulation material to facilitate understanding and real implementation in the field, namely Client computers 1 and 2 by carrying out various attacks such as flooding with TCP, ICMP, and UDP protocols against the server. Then analyze the response time of the attack detection test results. Internet Protocol (IP) block testing or intruder prevention manually using iptables. This research aims to realise a computer network on a good LAN network and has a network security system to detect and prevent attacks or intruders. It was then knowing the accuracy of the snort server in providing attack alerts detected by the IDS system based on the Snort Rule and the Intrusion Prevention System (IPS) system with iptables as a firewall can block the attacker's IP so that the attacker's client cannot attack.

Based on previous research on Snort, Marta et al (17) state that server security is an important thing that needs to be given more attention when configuring a server. In general, attacks on the server are known after the failure of the server to provide services. In this study, a server security system was built that can monitor a server when abnormal activity is detected.

Notifications will be sent via SMS (Short Message Service) to the network administrator's cellphone. The system built performs intrusion detection on the server in real-time using SNORT. When improper access occurs to the server, SNORT will detect and send information on the occurrence of unusual activity to the network administrator. This system was tested with five attacks: PING Attack, DoS/DDoS Attack, Port Scanning, Telnet Access and FTP Access. This study observes activity loads on server resources, including CPU, Memory (RAM) and network loads. The results show that when there is an attack attempt on the server, in another study from Efendi (20), Network security is an aspect that network administrators constantly improve, either by optimizing hardware or software. Snort is a detection sensor for network abuse, this system functions as a snort NIDS (Network Intrusion Detection System), which detects any intrusion attempts (intrusion).

Detection is carried out based on the rules that the administrator has described in the directory rules contained in the configuration file. Snort can analyze real-time alerts, where the mechanism for entering alerts can be in the form of a user Syslog, file or database so that it can detect attacks on computer networks early. Research from Hafiz et al. (13) explains that a backdoor or also called a back door, is special access made by an attacker to be able to re-enter a system that has been compromised. Most website owners ignore the security system due to a lack of knowledge about security or management personnel, so it is advantageous for an attacker to enter the system easily. Therefore, there needs to be a security system that can detect backdoors because the consequences are terrible for the system.

This system is called an intrusion detection system, while the most widely used is Snort IDS. This security system is based on a website that can detect security holes, one of which is the presence of a backdoor. Gunawan, Sastra, & Wiharta (21) explained that the Snort system could detect 250,519 total network data with 22 attributes and 212 types of network traffic. Snort system data is grouped by working hours and outside working hours. The Honeypot system can block up to 248,574 attacks and 10 types of attacks, each of which has an attacker's IP address. Therefore, it can be concluded that the use of snort and honeypot systems in this research application is very accurate and can be used to detect and prevent attacks on the Udayana University network.

Methods

The research method is carried out through several stages, as shown in Figure 1, where this process starts by determining the attack model (TCP, UDP, and ICMP). Then, it will determine the number of attackers from SIMRS that are simulated, the results of the attacks carried out will output in the form of the length of the process of the attack being carried out, the number of attack warnings that occurred is used as a result of accuracy. Snort is software that observes the activity in a network, which is open and free.

Figure 2 describes Snort as a package sniffing that uses tcp dump to take data packet images. By libcap will be separated to be forwarded to process Packet Decoder, Packet Decoder will separate packets from IP protocol, type package used. Then the preprocessor will analyze or select what package is that is whole or not. On Detection Engine, as center packet detection will be adjusted with rules signature if it matches, it will be until on the Output Stage which will be stored in the MySql database the result is report or alerts.

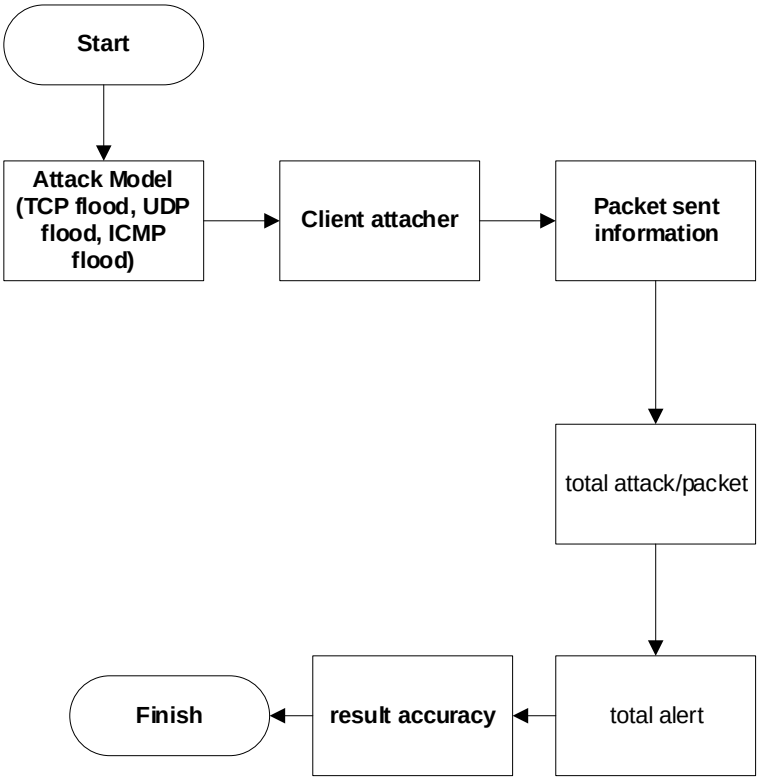

Figure 1.
Flow Research Method

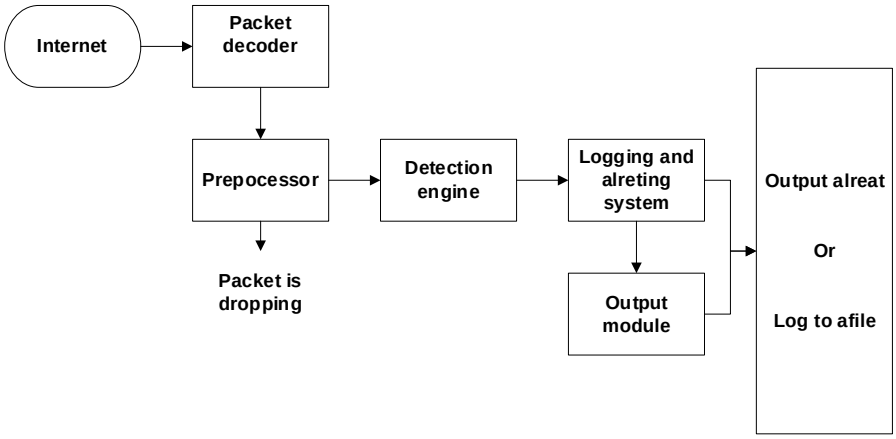

Figure 2.
Component functions in Snort (22)

The IP Tables work system filters data traffic and action with applied rules whether the package will be dropped, logged, accepted or rejected. In the IP Tables will be made rules (rule) for data traffic flow on a network into and out of the computer.

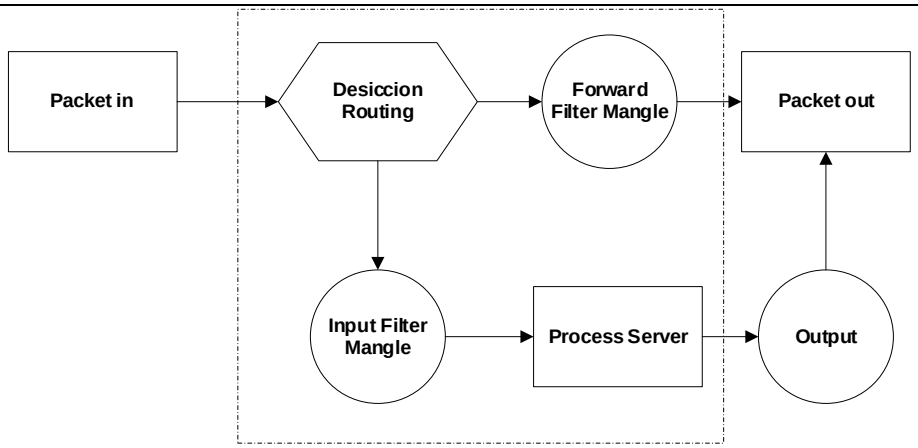

Figure 3.
System IP Tables Work (13)

Figure 3 explains the concept of IP Tables in receiving packets starting from the Incoming packet. Then it is processed based on the destination. If it is the destination IP of the firewall, it will go to the input process; if not, the destination IP for the firewall will be forwarded to the forward process. Finally, the next match based on the firewall's policy table is accepted or rejected. Intrusion Detection System (IDS) is activity-detecting devices that are suspicious on a network computer in real-time. Figure 4 describes the workflow of Intrusion Detection Systems (IDS) in detecting suspicious activity or intruders. By taking data packets on a computer network, detection will be carried out using Snort Rules-Based; if detected, it will give a warning and store data in the MySQL database. If no suspicious activity is detected, the process is complete.

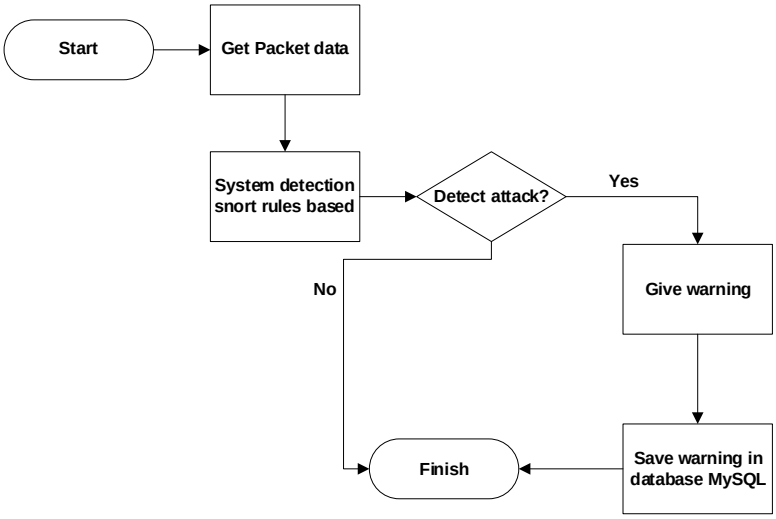

Figure 4.
Principle Intrusion Detection System (IDS) work (17)

Intrusion Prevention System (IPS) is a good security device that can detect any activity that is suspicious and prevents the activity. Figure 5 describes Intrusion Prevention Systems (IPS) 's work detecting and preventing suspicious activities. Snort Rules-Based detection will be carried out by taking data packets on a computer network. If detected, it will create a warning and save the data on the web application. Furthermore, IPS will block the passing packets by giving rules on IP Tables or firewalls.

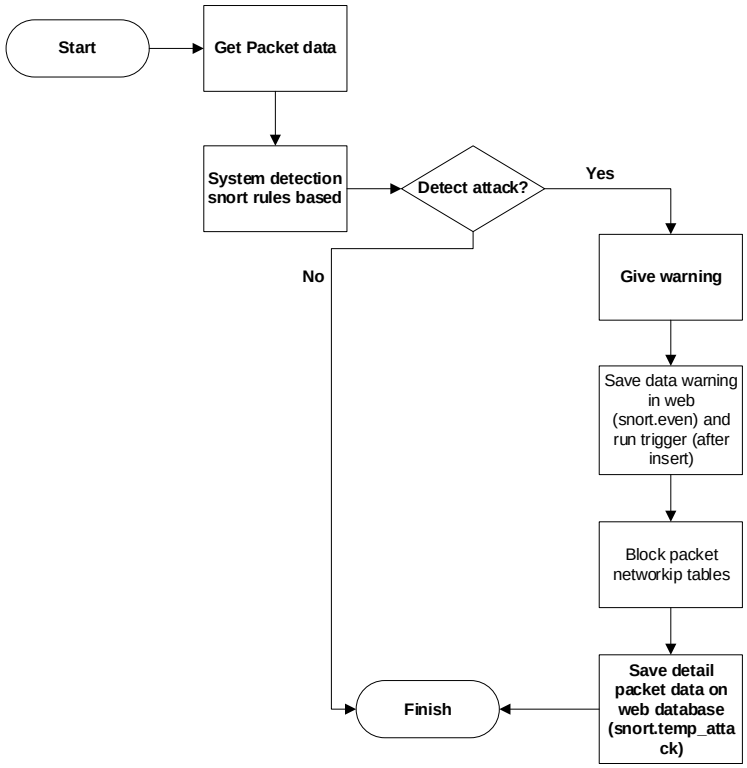

Figure 5.
Intrusion Prevention System (IPS) method flow (21)

Results and Discussion

In the research method in Figure 1, the researcher performs a simulation of Attack Detection System Testing (IDS) on the Snort Server with 1 Client. Testing is performed by client 1 acting as the attacker. Client 1 attacks the server with various attacks, namely flooding or flooding IP or Port using 3 Ports/Protocols, namely 22/TCP flood, 68/UDP flood, and ICMP floods.

Table 1 describes the design of the IDS system test. In this test, on 2 0/0 1/20 22 starting from 0 9 : 0 7:2 1 WIB to 1 4 : 1 8:0 5 WIB. By carrying out a flooding attack or flooding TCP/22 port with send data package of 1000 packets and 1 data package containing 1 attack, the result alerts detected on website BASE snort equal 1000. The test it reaches 100% yield.

Table 1.
Snort Intrusion Detection System (IDS) test table

Attack Model	Client Attacher	Packet send	total attack/packet	Total Alert	Result accuracy
TCP flood		1000	1	1000	100%
UDP flood	1	3000	2	5993	99.97%
ICMP flood		6000	2	12000	100%

On the attack model port 68/UDP port flooding with provides data packets of 3000 packets and 1 there are 2 data packets from the UDP port attack, alert results detected on website BASE snort for the UDP port of 5993 alerts, then the test on the model UDP achieved a 99.9 6 % yield. And the Ping/ICMP attack model has carried out flooding IP by delivering data of 5000 packets and 1 ICMP packet. So there are 2 attacks. The alert results are detected on the web BASE snort of 12 000, then testing on UDP models flood achieve 100%. So this response time analysis is an analysis of server response time by rules snort to an attack package done by 1 attacker client together with 3 attack models that is TCP Flood, UDP Flood, and ICP Flood can be seen in Table 2.

Table 2.
Response Time Rules Snort

Attack Model	Time Span	Total Packet accept	TCP Response Time
TCP flood	1050,335 s	1370	0.72 s/packet
UDP flood	2581,886 s	5798	0.54s/packet
ICMP flood	5398,634 s	15879	0.44 s/packet

Table 2 is the result of response analysis time server by snort rules in detect when there is an attack package that given by 1 attacking client. For TCP attack model flood generate time span 10 5 0.335 s/total package 1 3 70=0. 7 2 s/packet, UDP flood generate time span 25 8 1,886 s/total package 57 9 8=0. 5 4 s/package, and ICMP Flood produce time span 5 3 9 8 .634 s/total package 158 7 9 = 0. 4 4s/package.

Attack Detection System Testing (IDS) with two clients, namely with a simulation scheme that acts as an attacker. Client 1 and Client 2 perform attacks automatically against servers with variations that are flooding or flooding IP or Port using 3 Port/Protocol.i.e. 22/TCP flood, 68/UDP floods, and ICMP floods. Table 3 explain the test plan IDS system. In this test, On 23/0 1/20 22 starting at 1 4: 1 0:32 WIB until 1 7: 1 8:32 WIB with 2 clients doing flooding attack or port flooding TCP/22 simultaneously.

Table 3.
Snort Intrusion Detection System (IDS) Testing

Attack Model	Client Attacher	Packet send	total attack/packet	Total Alert	Result accuracy
TCP flood		1000	1	2000	100%
UDP flood	2	3000	2	9998	99.97%
ICMP flood		6000	2	12000	100%

By sending a data packet of 1000 packets and 1 data packet containing 1 attack, alert results were detected on website BASE snort of 2000 alerts. Then this test reached 100% yield. On port 68/UDP attack model done by 2 clients at the same time perform a port flooding attack with provides data packets of 3000 packets and 1 data packet from port UDP has 2 attacks, alert results are detected on web BASE snort for UDP port as big as 999 8 alerts. The test on UDP l mode achieves 99.9 7 % results. And models Ping/ICMP attack carried out 2 clients directly simultaneously do flooding IP with providing data package of 6 000 packages and 1 ICMP package there were 2 attacks. The results of which alerts were detected on the BASE snort web were 1 2000 alert, then testing on the model UDP flood reaches 100% yield.

Conclusion

SIMRS network security simulation using snort on network security system LAN capable of being integrated well and can be tested well. IDS System with the Snort implemented can do detection attack with the average result the accuracy value the same is 99.97 % on testing with 1 client and 2 clients. The generate average Mark response time server by rules snort which good that is less than 1-second read package existing data, at the time testing with 1 client which is 0.5 0 second and with 2 clients namely 0.32 second. Researchers realize that this network security simulation, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) have good results. However, they are not optimal because it has not been implemented in actual hospitals. Therefore, developing a better Intrusion Detection System (IDS) system to detect more attack models and an Intrusion Prevention System (IPS) that can block IP attacks automatically is necessary.

Reference

1. Pujihastusi A, Hastuti NM, Yuliani N. *Penerapan Sistem Informasi Manajemen Rumah Sakit dalam Mendukung Pengambilan Keputusan Manajemen*. J Manaj Inf Kesehat Indones. 2021;9(2):191–200.
2. Safii M, Zulhamsyah A. *Sistem Pendukung Keputusan Pemilihan Mekanik Sepeda Motor Yamaha*

Alfascorfii Dengan Metode Multi Objective Optimization On The Basis Of Ratio Analysis (MOORA). J-SAKTI (Jurnal Sains Komput dan Inform. 2018;2(2):162.

3. Harsono A. *Sistem Informasi Manajemen Rumah Sakit Umum Daerah (SIM-RSUD) Terintegrasi Di Provinsi*. Eksplora Inform. 2015;5:11–22.
4. Acai Sudirman, Muttaqin Muttaqin, Ramen A. Purba, Alexander Wirapraja , Leon A. Abdillah, Fajrillah Fajrillah, Fatimah Nur Arifah, Julyanthry Julyanthry, Ronal Watrianthos JS. *Sistem Informasi Manajemen*. Yayasan Kita Menulis; 2020.
5. Andriani R, Kusnanto H, Istiono W. *Analisis Kesuksesan Implementasi Rekam Medis Elektronik Di Rs Universitas Gadjah Mada*. J Sist Inf. 2017;13(2):90.
6. Febriani Y. *Sistem Informasi Pengelolaan Data Pasien Rawat Jalan Klinik Pratama Anugrah Demak Berbasis Web Dengan Notifikasi Telegram*. Sitech. 2020;Vol 1, No:1–6.
7. Islamy IT, Astuti HM, Wibowo RP. *Perancangan dan Pembuatan Sistem Pelaporan Kinerja Berbasis Online untuk Pranata Komputer*. JUITA J Inform. 2020;8(1):91.
8. Katarina D, Ambarsari EW. *Profile Matching Sebagai Evaluasi Implementasi Sistem Informasi*. Semnas Ristek. 2018;123–8.
9. Pekalongan DIK. *Sistem informasi layanan kesehatan berbasis mobile yang mengintegrasikan instansi layanan kesehatan di kota pekalongan*. 2016;11.
10. Suryadharma, Budyastuti T. *Sistem Informasi Manajemen*. Ponorogo: Uwais Inspirasi Indonesia; 2019.
11. Noor MF, Pambudi YD, Widiyanto WW. *Analisa Alur Proses Penentuan Kebutuhan Sistem (Studi Kasus: Sistem Informasi Pengolahan Raport)*. J Inf Politek Indonusa Surakarta. 2018;4(1):20–6.
12. Simanjorang RM, Hutahaean HD, Sihotang HT. *Sistem Pendukung Keputusan Penentuan Penerima Bahan Pangan Bersubsidi Untuk Keluarga Miskin Dengan Metode Ahp Pada Kantor Kelurahan Mangga*. J Inform Pelita Nusant [Internet]. 2017;2(1):22–31. Available from: http://e-jurnal.pelitanusantara.ac.id/index.php/JIPN/article/view/274/172
13. Hafiz A, Kurniawan T, Sivi NA, Ikhsan FK, Andhika P. *Analisis Celah Keamanan Jaringan Dan Server Menggunakan Snort Intrusion Detection System*. J Inf dan Komput. 2020;8(2):59–66.
14. Surahmat, Novaria Kunang Y, Erlansyah D. *Analisis Keamanan Sistem Wpa Radius*. Anal Keamanan Sist Wpa Radius Surahmat1. 2016;177(0711):515679–124.
15. Zulhalim, Rachmawaty Haroen AF. *Berbasis Mobile Hybrid Pada RSUD Kemayoran*. 2020;4(2):97–114.
16. Awajan AM, Ismail MT, Wadi S Al. *Improving Forecasting Accuracy for Stock Market Data using emd-hw Bagging*. PLoS One. 2018;13(7):1–20.
17. Marta IKKA, Hartawan INB, Satwika IKS. A*nalisis Sistem Monitoring Keamanan Server Dengan Sms Alert Berbasis Snort*. Inser Inf Syst Emerg Technol J. 2020;1(1):25.
18. Akhriana A, Irmayana A. *Web App Pendeteksi Jenis Serangan Jaringan Komputer Dengan Memanfaatkan Snort Dan Log Honeypot*. CCIT J. 2019;12(1):85–96.
19. Agustin R, Fitri I, Nathasia ND. I*mplementasi Metode Intrusion Detection Systems (IDS) dan Intrusion Prevention Systems (IPS) Berbasis Snort Server Untuk Keamanan Jaringan LAN*. J Inform. 2018;18(1):71–84.
20. Efendi TF. *Analysis of the Implementation of the Simple Salary Sim Application in Grogol District, Sukoharjo*. 2020;2020(4):1363–72. Available from: https://jurnal.stie-aas.ac.id/index.php/IJEBAR/article/view/2303/1074
21. Gunawan AR, Sastra NP, Wiharta DM. Penerapan Keamanan Jaringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware. Maj Ilm Teknol Elektro. 2021;20(1):81.
22. Efendi NP. *Sistem Keamanan Jaringan Menggunakan Snort*. 2019.