The 2nd Conference on Management, Business, Innovation, Education, and Social Science (CoMBInES)

Taichung, Taiwan 3-6 March, 2022

DESIGN AND EVALUATION OF CLOUD COMPUTING NETWORK SECURITY USING NETWORK DEVELOPMENT LIFE CYCLE METHOD AT PT. XYZ

Gautama Wijaya, Franky Viky Franklyn

Faculty of Computer Science, Universitas Internasional Batam

{Gautama@uib.ac.id , 1831189 .franky@uib.edu }

ABSTRACT

Cloud computing is an internet-based service model for accommodating enterprise resources where companies do not have to think about resources because cloud computing service providers provide resource facilities on the internet. Because the resources of cloud computing systems on the internet, as well as providing services to many people simultaneously, can allow cloud computing systems to be easily threatened by various types of Cyber Attacks. The purpose of this research is to develop the design of a secure cloud computing network architecture using the NDLC method by developing a cloud computing network security system using IDPS case study technology at PT. XYZ. IDPS Snort is used as an intrusion detection and prevention system as well as a firewall to filter packet packets that are indicated as threats. The evaluation was conducted to prove whether the network security system applied to cloud computing technology can run well, by testing several attacks such as Ports Scanning using NMAP, Ping of Death and DoS SYNFlood. The results of the evaluation proved that IDPS SNORT can detect and block all well-tested attacks on the applied cloud computing network.

Keywords: *Cloud Computing, Network Security, NDLC, IDPS*

INTRODUCTION

Today, information technology in the world has experienced a very rapid increase, with technological developments that are found to increase the effectiveness and efficiency of human activities. All activities from waking up to sleeping now cannot be separated from digital activities, in the future humans will only have to enjoy all these digital works without having to bother to think about them.(Danuri, 2019).*Cloud Computing*is one form of information technology development that we are now living. Cloud Computing is an internet-based service model to accommodate a company's resources, which means the company no longer needs to think about infrastructure because Cloud Computing service providers provide storage facilities on the internet. Cloud Computing can provide unlimited services for users to access applications without any time, place and distance limits. There are three types of services contained in this Cloud Computing technology, namely, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Cloud Computing scientifically means a method that allows users to rent an information technology service such as software, processing power,('Abidah et al., 2020).Utilization of cloud computing can be more optimal if the organization or company that uses it is more considerate of the type of service used so that it is not overcharged or that the excess technology does not meet its needs. so that this cloud computing technology can really support the company's capabilities, it is necessary to carry out the right analysis according to the company's needs(Bahri, 2019)Because Cloud Computing system resources are located on the internet, as well as

providing services to many people at the same time, it can allow Cloud Computing systems to be easily threatened by various kinds of *Cyber Attacks*. So to overcome the attacks that may appear on the Cloud Computing network can be done using Intrusion Detection System (IDS) technology. IDS is a security system where if there is any suspicious behavior that is not in accordance with the rules applied to the network, the IDS will provide alerts and if possible block the IP address that carried out the attack.(Syani, 2019).Intrusion Detection and Prevention System (IDPS) technology is a development of the Intrusion Detection System (IDS) which is combined with a firewall in this case using IP Tables. In some previous studies on IDPS, the main purpose of IDS is to detect attacks efficiently. In addition, it is equally important in detecting attacks to reduce their impact. The application of the Intrusion Detection and Prevention System (IDPS) is used as a solution that can be used to assist administrators in monitoring and analyzing malicious packages contained in a network.(Alamsyah et al., 2020).Based on the description above, the author intends to design and evaluate network security or a network security system for a cloud server network using intrusion detection and prevention system technology with software called SNORT as a network security tool by taking a case study of a server network at PT. XYZ and network development life cycle as the design method. In the design of this network security system, it is hoped that it will make it easier for users to monitor cloud server networks and speed up users for handling server downs or attacks that may appear on the cloud server network.

PROPOSED INNOVATION

Research byIrawan, Sari & Bahri, (2019)talk about the design or design of a cloud computing storage technology or what is commonly called cloud storage. As a model of cloud computing, cloud storage provides services for file management based on users in a computer network. The author uses Nextcloud as a cloud server application that is suitable for running cloud storage services, Nextcloud can share files to all users and share via a link via the web. To run and configure Nextcloud, it can be accessed via a web browser by going to the Public server IP address.

Research bySyani & Ropi, (2018)analyze and build a cloud computing infrastructure network security system with case studies in the education sector where cloud infrastructure is built based on user needs obtained from direct interviews. The author uses the NDLC methodology which consists of 5 stages with test results showing that the network security system built has been successful and the implemented cloud system meets user requirements. The resulting performance on the system detection accuracy parameter can detect attacks accurately and quickly, while the system resource parameters take very little CPU and RAM usage so that it does not burden the server. Observations made by the author showed good results with as many as 620 surveillance warnings, Next on researchEka Stephani, (2020)about evaluating the performance of attack detection on IDPS Snort. This study evaluates the performance of an IDS, namely SNORT based on several factors, namely the ability to detect attacks directed at the host, CPU and memory resource consumption by SNORT when detecting multiple attacks from several attackers. Based on the test results, it is concluded that SNORT can detect attacks in accordance with the signature that has been set in the SNORT rules which then if an attack is detected in accordance with these rules it will be reported via notification in a time span of 2 seconds to 139 seconds. SNORT has a reliability of up to 100% for types of attacks such as Port Scanning, SSH Bruteforce and DNS Enumeration. Other research conducted by Rakhman & Lestariningati, (2015)about IDS design using SNORT software. This study designs a server using the Linux Ubuntu 13.10 operating system then installs and configures SNORT as a web server network security and then tests the SNORT Server by attacking the web server with several attack techniques that hackers usually do against a network, namely DoS (Denial of Services).) and SQL Injection. The server is activated for 506 hours per day for 6 days and attacks are carried out randomly

every day. In functional testing of the IDS server, the existing functions run according to the design that has been built, SNORT is able to detect attacks that appear and display warnings to the administrator, there are a total of 128. 576 warnings of which 51 are DoS attack warnings and 678 of which are SQL Injection attack warnings. The IDS in this study which is implemented on the Linux Ubuntu operating system can monitor events on the network and the SNORT Web UI used is very helpful for the network monitoring process because it is GUI based.

Research byAulia & Hariyadi, (2016)discusses the implementation of an intrusion prevention system (IPS) using Snort and IPTables for cloud computing network security. This study focuses on cloud network security with SaaS (Software as a Service) services where the cloud provider provides software that can be used and can be accessed by users via a web browser. The methodology used in this research is NDLC (Network Development Life Cycle). This research applies a cloud computing network by virtualizing it on Virtualbox, the author applies IPS Snort which is integrated with IPTables successfully detects, displays notifications and blocks the 4 attacks that were tried, namely Ping Attack, Port Scanning, Sniffing and DOS SYNFlood Attack for 5 trials.

METHODS

In preparing this thesis the author uses a research method called the Network Development Life Cycle (NDLC) method. This method is used as a guide in a series of computer network development processes. NDLC formulates the circulation of the process of compiling or building a computer network system(Kurniawan, 2016). NDLC has six hierarchies that serve as guidelines for implementing it on the network. The six hierarchies in question are Analysis, Design, Simulation Prototyping, Implementation, Monitoring, and Management as shown in Figure III.2(Nurdadyansyah & Hasibuan, 2021).

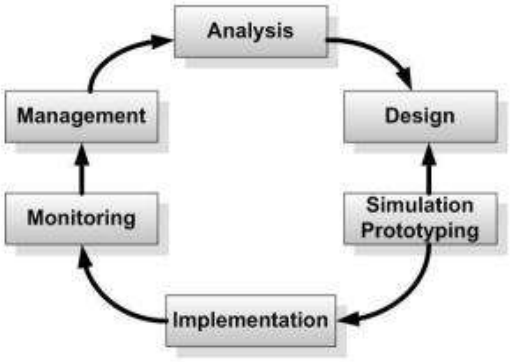

Figure 1. NDLC

RESULT AND DISCUSSION

4.1 ***Analysis***

4.1.1 Existing network analysis

Analysis of the state of the network or network architecture that already exists for research partners to be analyzed and developed to be more optimal according to existing needs. The results of the analysis related to the network at PT. XYZ are shown in Figure IV.1 below. Where the existing network still adopts a physical network with the server still a physical device, the PC server provides Web Server, File Server, Mile Server and Database Sever services. From the results of the analysis of the network is still vulnerable to attacks by attackers because they do not have a good network security system.

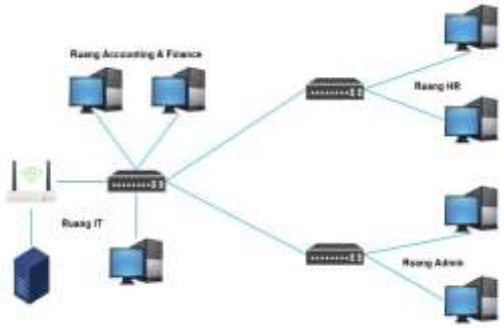

Figure 2. Network Topology

4.1.2 Workflow design

The flow of the work process of the network security system from IDPS SNORT that will be made is shown in Figure IV.2. Where every packet that enters the system will be captured first, then the data packet will be checked or detected

based on the rules that have been made, if the packet is indicated as a threat or detected according to existing rules, the system will warn the administrator and record The log of the data packet will then also block the data packet because it is indicated as an attack. However, if a data packet is detected that does not comply with the violated SNORT rules, the system will log the data packet and continue it to the cloud computing server.

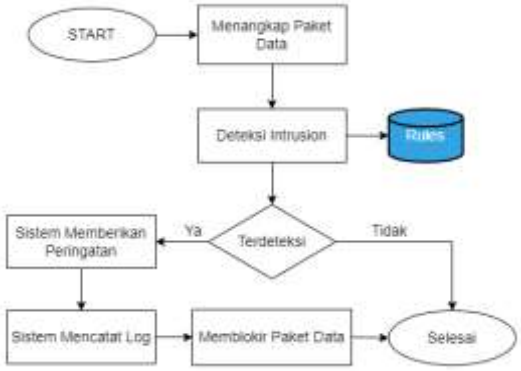

Figure 3. System Workflow

4.1.3 Research instrument design

To support the design of the trial network that is made, analysis is needed regarding user needs as well as the hardware and software needed in the network design:

A. User Needs

The needs for users are obtained by conducting field surveys using the interview method. With the results of the interviews obtained the following needs:

- The system to be designed aims to detect and monitor network activity on the personnel server, this server is used to perform data management, personnel management and administration with ports that are opened including port 80 (HTTP), port 22 (SSH), port 3306(MYSQL).
- The security system or network security system designed is expected to be able to detect if there is a threat and block it, and can monitor any changes that appear on the server.

B. Hardware Requirements

As for the specifications*hardware*needed in this research design are as shown in Table 3 below:

Table 1. Hardware Specifications

Device		Specification	
		Cloud Server	*Client*
PC	1. RAM (Random Access Memory)	4GB	2GB
	2. *Processor*	2 GHZ	2 GHz
	2. *Storage*	50GB	200GB
Network	1. *Ethernet Card*	*Cloud*	*Wifi Adapter*

C. Software Requirements

As for*software*used in testing this system is as shown in Table 2 below:

Table 2 Software Specifications

No	***Software***	**Version**	**Information**
1	Ubuntu	20.04.4 LTS	Operating System used on the Personnel server
2	PuTTY	0.76	For SSH Client
2	SNORT	2.9.7	IDS server application
3	IPTables	1.8.4	Traffic filter to block attacks
4	Kali Linux	2020	The operating system used on the attacker's device
5	Wireshark	2.4.2	Applications used as packet sniffing

4.2 ***Design***

In the design stage the author designs a cloud computing-based network architecture using a website application called draw.io, in this design process the author makes designs according to user needs using the Amazon web service (AWS) cloud provider. And also add a network security system design as network security that will be implemented to avoid attacks on servers.

4.3 ***Implementation***

In the implementation stage, this is the stage where the author applies and configures the cloud architecture design and network security system that has been previously designed for further evaluation at a later stage. Implementation begins with configuring a cloud server using amazon web services (AWS).

4.3.1 VPC (Virtual Private Cloud) network installation

- Log in to AWS then search for the VPC management console and create a new VPC, here the author creates a virtual computer network so that various cloud resources in AWS such as EC2 instances, RDS instances, S3 Buckets can be isolated from the internet to make it more secure. Here the author determines the IP CIDR block 10.10.0.0/16 as the IP range used in this virtual network.

Figure IV.3 Create a VPC

- Next, create 2 subnets for the newly created VPC, the subnets are used to determine public and private IPs with these subnets being in the same availability zone, namely ap-southeast-1a (Singapore). The public IPv4 CIDR 10.10.1.0/24 and private IPv4 CIDR 10.10.2.0/24 ranges each have 250 available IPs.
- Then create an internet gateway and connect it to the previously created VPC so that it can be accessed by the internet.
- Set the routing table of the VPC to direct the network packet 0.0.0.0/0 to the internet gateway, as well as link the previously created subnets so that they are connected to each other, both public and private.
- Next, create a security group for security on the VPC network so that not all packets can enter the server, determine what ports are open and the IP range or the rules for entering and leaving packets.

Figure IV.4 Create Security Groups

- Set elastic IP so that the Public IP address on the web server does not change when the machine instance is turned off.

Figure IV.5 Create Elastic IPs

4.3.2 S3 Bucket Installation

- Creating an Amazon S3 bucket that is used as a storage medium on the AWS S3 internet focuses on file management where we can create a bucket (bucket) as a container to insert files, then upload files to the bucket, manage the files so that anyone can access them.
- Create a bucket then specify the AWS region (zone) here the author defines Asia Pacific (Singapore) ap-southeast-1. Then try uploading the file or document to the created bucket. As in the image below.

Figure IV.6 Create S3 Bucket

4.3.3 EC2 Instance Installation

- Create an EC2 instance as a virtual machine that is used as a web server

with specifications as designed according to system requirements.

Figure IV.7 Create EC2 Instance (web server)

- Next, enter the instances that have been successfully created, here the author uses the SSH PuTTY application to connect to instances or can also directly connect via the AWS web. Then copy the folder in the form of the application source code file that we uploaded earlier on the s3 busket, but first install the AWS CLI on the instances, then type the command $ aws s3 sync s3://bucket_name/folder_name.

4.3.4 Web Server Installation

- Then install apache as an application or web server tool, do an update and upgrade first on the instance, after that install apache, php and also mysql server as the admin database.

Figure IV.8 Install apache

- After the web server has been installed, we configure the database and application so that when users access the Public IP server, they will go directly to the application, to facilitate database creation, we also install phpMyAdmin. Once connected, the web server has been successfully built for later analysis of the security system.

Figure IV.8 Successfully Installed Web Application

4.3.5 Network Security System Installation

- After the web server configuration is complete and running well, we can install and configure the network security, this time the author uses IDS Snort as an application to detect packets in the form of attacks and record them as a log.

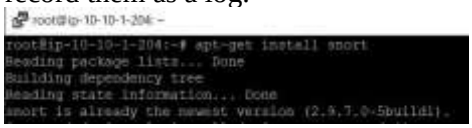

Figure IV.9 SNORT . Installation

- After the installation process is successful, proceed with configuring the rules database on Snort to detect attacks and display alerts. Here are some examples of rules that the author applies.

Figure IV.10 Example of SNORT . rules

- After the detection system is successfully implemented, it is followed by an attack prevention system that will block packets that are detected as an intrusion. Installing iptables as a firewall application on the web server as follows.

Figure IV.11 Installation of IPTables

- After the detection and prevention system has been successfully implemented, then proceed with the testing phase for intrusion attacks.

4.3.6 Attacker Installation

- At this stage the author prepares a virtual machine that is used as an attacker's device. The author uses the VirtualBox application to install the Kali Linux operating system as an attacker device.

Figure IV.12 Attacker Device Installation

- Next, update && upgrade the Kali Linux operating system to install the package or application needed as an attacker.

4.4 Test

This stage is the stage where the network security system that has been built will be tested with several repeated attacks and then evaluated whether the security system is running well.

4.4.1 *Port Scan (Nmap)*

*Port Scan*is an experimental activity to observe the server to find out which hosts are active, what ports are open, the operating system used and other scanning features. The following is an example of an attack test performed using the nmap tool. nmap tests the attacker's computer before the network security system blocks its activity.

Figure IV.13 Port Scanning Experiment Successful

It can be seen from the observation that port scanning was successful before snort and iptables blocked. By doing port scanning attackers can find out which ports are open and which can be accessed. It can be seen in the picture above that port 22 (ssh) and port 80 (http) are open and can be accessed.

- Network traffic monitoring using wireshark shows that there is a packet request to the IP server via the TCP protocol.

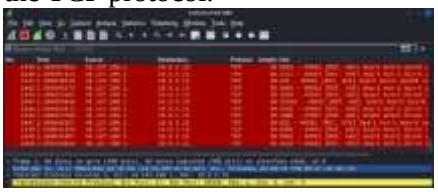

Figure IV.14 Wireshark Sniffing Packet NMAP

- Snort condition in detection mode there is an alert that is an attack attempt.

Figure IV.15 Snort Detects NMAP

- Configure iptables rules to block port scanning attacks.

Figure IV.16 IPTables Rules Block Port Scanning

- Retry port scanning using nmap to see if iptables was successful in blocking the attempted attack.

Figure IV.17 Successful Port Scanning Experiment

It can be seen in the picture above that the port scanning experiment

was successful, but the port that was open is now closed so that it cannot be exploited by attackers.

- The following is a log of the attempted port scanning attack carried out by the attacker.

Figure IV.17 Port Scanning Experiment Log (NMAP)

4.4.2 *Ping Of Death*

*Ping Of Death*is a form of attack in the form of sending packets in large numbers to the server to burden server performance through the icmp port.

- The icmp attack from the attacker's device by sending as many as 10000 times the request to the server.

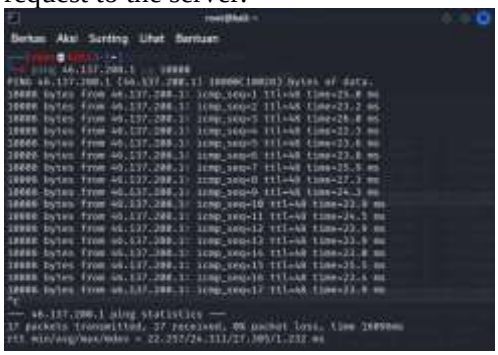

Figure IV.18 Closed Port Scanning Experiment

It can be seen in the picture above that all packets sent to the server were successfully sent with 0% packet loss.

- Seen in wireshark ping of death packet requests via the icmp protocol.

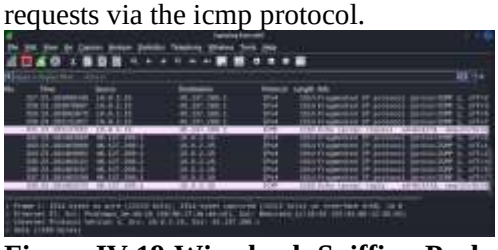

Figure IV.19 Wireshark Sniffing Packet Ping of Death

- Furthermore, it can be seen that the snort detection mode sends an alert in the form of an attempted ping of death attack as shown below.

Figure IV.20 Snort Ping of Death Detection

- Then create rules to block ping of death attacks by limiting the number of packets that the server can receive.

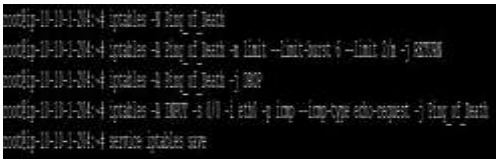

Figure IV.21 IPTables Rules Block Ping of Death

- Then a ping of death experiment was carried out again from the attacker's device to find out whether this activity could be prevented.

Figure IV.22 Ping of Death Attempt Failed

The picture above shows that the attack attempt was in the form of sending 10000 undelivered packets to the server, with 95.45% packet loss.

4.4.3 *SYN Flood*

*SYN Flood*is a form of attack such as DoS (Denial of Service) where the attacker will send a large number of SYN requests to the target server which aims to overload the server resources so that it cannot serve traffic properly.

- Attempts to attack SYN packets from the attacker's device using a tool called hping3.
- We can see in wireshark the number of attack attempts with large packets over port 80 and we can see an unusual spike in traffic.

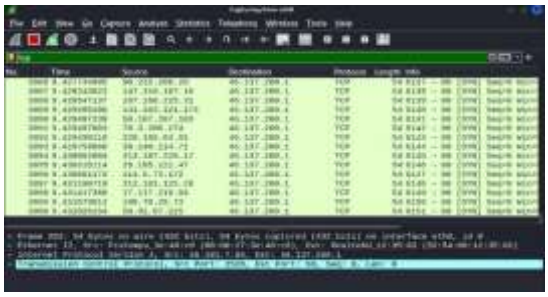

Figure IV.17 Wireshark Sniffing Packet SYN Flood

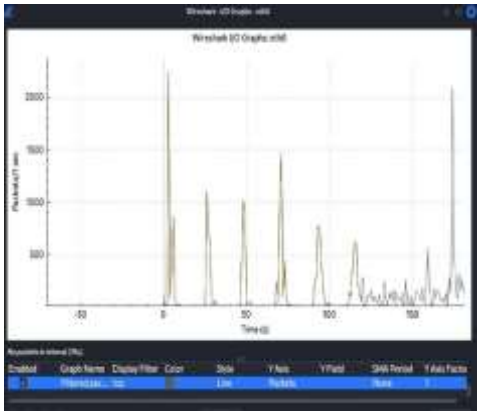

Figure IV.17 Wireshark Traffic Graphs SYN Flood

- It appears that snort can detect a SYN Flood attack and display alerts and the attacker's IP.

Figure IV.17 Snort Detect SYN Flood

- With these alerts then a rule is created to prevent these attacks so that server resources are not down.

Figure IV.17 IPTables Rule SYN FLOOD

- Furthermore, the SYN Flood attack experiment is returned by the attacker's device to determine whether the attack prevention system is functioning properly or not.

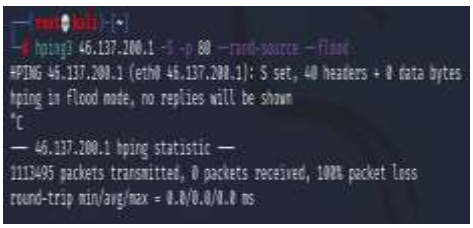

Figure IV.17 SYN Flood Trial Failed

Seen in the picture above all packets sent to the server are not sent.

4.5 Evaluation

At this stage the network security system will be evaluated whether it is running well according to the needs, where snort can capture packets in the form of attacks and block them from entering the server. From the conclusion of the security results applied, cloud computing is currently flexible because the proper configuration at the beginning of its implementation creates a mechanism that is activated automatically and complements cloud computing so that it is more flexible in securing the network.

Table 3 Test Results Against The System

Attacker	***OS***	**Attack**	**Tools**	**Snort**
36.77.145.212	Kali Linux	Port Scanning	NMAP	✓
		Ping Of Death	ICMP	✓
		SYN Flood	Hping3	✓

Conclusion

Using the Network Development Life Cycle NDLC development method is proven to build a secure network architecture design to be applied to cloud computing technology. Because in the design process is more structured and each stage can be easily done. The 3 stages that the author uses, namely analysis, design and implementation can run well and successfully develop a cloud computing network architecture for the needs of a secure web server for the company.To implement this cloud architecture design the author took a case study on PT. XYZ, from the

network topology and systems that have been running the author performs the analysis then redesigns it to be applied to cloud computing technology. The design carried out includes the design of system workflows and the needs of system devices so that a network architecture design is obtained that suits the needs of PT. XYZ at the moment. Network security implemented by IDPS Snort and firewall successfully detect attacks and block them, has previously been configured and added rules to be able to detect and display alerts and block packages indicated as attacks. Evalusai in the form of test results on the IDPS Snort security system can be seen on table 3. Idps Snort detected 1 IP address (36.77.145.212) using the kali linux operating system and successfully detected the attack packages namely Port Scanning, Ping of Death and SYN Flood and blocked them so that the IP could not exploit the server again. With this IDPS Snort is considered good enough to secure and analyze the form of intrusion attacks into cloud computing network systems.

REFERENCES

'Abidah, I. N., Hamdani, M. A., & Amrozi, Y. (2020). Implementasi Sistem Basis Data Cloud Computing pada Sektor Pendidikan. *KELUWIH: Jurnal Sains Dan Teknologi*, *1*(2), 77–84. https://doi.org/10.24123/saintek.v1i2.2868

Alamsyah, H., -, R., & Al Akbar, A. (2020). Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System. *JOINTECS (Journal of Information Technology and Computer Science)*, *5*(1), 17. https://doi.org/10.31328/jointecs.v5i1.1240

Aulia, D., & Hariyadi, I. P. (2016). *Analisis Penerapan Intrusion Prevention System (IPS) Menggunakan Snort dan IPTables untuk Keamanan Cloud Computing Software as a Service (SaaS)*.

Bahri, S. (2019). Analisa Kebutuhan Cloud Computing Dalam Mendukung Bisnis Perusahaan. *Informatic Engineering and Science Journal*, *9*(2), 1–4.

Danuri, M. (2019). Development and Transformation of Digital Technology. *Infokam*, *XV*(II), 116–123.

Eka Stephani, S. (2020). Jurnal Ilmiah Kohesi Vol. 3 No. 1 Januari 2019. *JURNAL ILMIAH KOHESI*, *4*(1), 124–128.

Irawan, A., Sari, A. P., & Bahri, S. (2019). Perancangan Dan Implementasi Cloud Storage Menggunakan NextCloud Pada Smk YPP Pandeglang. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *5*(2), 131–143.

Kurniawan, R. (2016). Analisis Dan Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode NDLC (Network Development Life Cycle) Pada BPU Bagas Raya Lubuk Linggau. *Jurnal Ilmiah Betrik*, *7*(01), 50–59. https://doi.org/10.36050/betrik.v7i01.12

Nurdadyansyah, N., & Hasibuan, M. (2021). Tampilan Perancangan Local Area Network Menggunakan NDLC Untuk Meningkatkan Layanan Sekolah. *Konferensi Nasional Ilmu Komputer (KONIK)*, 342–346.

Rakhman, A. A., & Lestariningati, S. I. (2015). Perancangan Ids Dengan Teknik Hids (Host Based Intrusion Detection System) Menggunakan Software Ossec. *The Journal of the Japanese Society of Clinical Cytology*, *34*(604), 1–7.

Syani, M. (2019). *Analisis Dan Implementasi Network Security System Menggunakan Teknik Host-Based Intrusion Detection System (Hids) Berbasis Cloud Computing*. *Selisik*. https://doi.org/10.31227/osf.io/6t7us