



## Network Security Analysis Using Virtual Private Network in Vocational School

**Yosi Nofita Sari\* , Dedy Irfan, Asrul Huda**

Postgraduate Vocational Technology Education, Faculty of Engineering,  
Universitas Negeri Padang

Corresponding Author. Email: [yosinofitasari1994@gmail.com](mailto:yosinofitasari1994@gmail.com)

**Abstract:** Every organization chooses a virtual private network (VPN) as their top option since it is a practical and secure solution. Through the use of a virtual private network, this study seeks to evaluate the network in SMK (VPN). The descriptive qualitative research used in this study was carried out at the lab of SMK Negeri 1 Ampek Angkek. Data were gathered through observation, interviews, and document analysis studies. The method of data analysis employed descriptive analysis. The results of this study indicate that the activity on the VPN network is better than the Non-VPN because the activities carried out in the VPN tunnel are not known by others. Users find it simpler to finish their daily agenda as a result.

### Article History

Received: 20-05-2022

Revised: 15-06-2022

Accepted: 23-06-2022

Published: 21-07-2022

### Key Words:

Network; VPN;  
Vocational School.

**How to Cite:** Sari, Y., Irfan, D., & Huda, A. (2022). Network Security Analysis Using Virtual Private Network in Vocational School. *Jurnal Paedagogy*, 9(3), 582-590. doi:<https://doi.org/10.33394/jp.v9i3.5346>



<https://doi.org/10.33394/jp.v9i3.5346>

This is an open-access article under the [CC-BY-SA License](https://creativecommons.org/licenses/by-sa/4.0/).



## Introduction

The internet, in particular, makes use of computer networks in the form of wired and wireless media (Noviansyah & Saiyar, 2020). Access to computer networks is a requirement that cannot be avoided. Computers are employed in the educational process as well; many schools have computer networks that connect local networks to the internet. The computer lab of SMK Negeri 1 Ampek Angkek, which is situated on Jl. Raya Panca, Batu Tabu, Kec. Ampek Angkek, Agam Regency, West Sumatra, provides instructional activities. The reason SMK Negeri 1 Ampek Angkek was chosen is because it offers sophisticated and modern educational opportunities, and all of its activities are supported by an online network. As a result, the facilities and network connections must be secure and simple in order to better support this. The school's internet network is currently regarded as being rather unsafe. Therefore, in order to support learning activities and several other issues, a stronger and safer computer network infrastructure is required. A LAN network is used for the computer network in the computer lab. This network is restricted to a rather small region, which is often not far from 1 sq km (Musalifa & Panu 2019). An essential component of managing computer networks is system security. Increased network access, which is required for education and other purposes, leads to data theft on the network, which depletes the network's resources (Sulaiman, 2016).

The internet network of SMK Negeri 1 Ampek Angkek still has a number of flaws, including users who only use one password protection, making it easy to identify them, no bandwidth sharing, and improper authentication, making it simple to attack them. The sluggish access speed indicates that the internet network is not consistent. Cybercrimes like spoofing, sniffing, phishing, denial of service attacks (DoS), and other security assaults are, of course, possible with these diverse flaws.

We require a network solution to solve this issue that is encrypted while yet operating on a public network. It's referred to as a virtual private network (VPN). The usage of a VPN to connect to a local network after initially connecting to a public network is described by



Putra and Anggraini (2018). Given that it may be a convenient and affordable solution for deploying data communications, VPN is actually the first choice for any organization (Ekawati & Irwan, 2021). By utilizing a VPN, the data is masked so that other users cannot access it, making it safer to use on a public network. By obscuring data transmission and altering the connection path through the server, access to the website is made safe (Mujiastuti & Prasetyo, 2021).

The purpose of this study is to use a virtual private network at SMK Negeri 1 Ampek Angkek to investigate network security. Prior to creating a computer network, analysis is required. This study can take the form of examining the existing network system, which includes issue analysis, requirements analysis, device analysis, and topological analysis so that data that will be used as a reference can be obtained (Mananggal, et al. 2021). This research is crucial to complete in order to improve network security in schools, such as the ability to encrypt data before it is sent over an internet network, preventing its contents from being read by careless parties. It is also crucial to manage users inside the school grounds for clients who have access to information that is typically only permitted in specific areas.

## **Research Method**

This study used a descriptive qualitative approach because all the data obtained were in the form of interviews and face-to-face results. Qualitative research aims to fully comprehend the phenomena of what study participants experience, including behavior, perception, motivation, action, etc., in a descriptive manner using words and language, in a particular natural context, and by applying diverse natural methodologies (Moleong, 2011). Based on observations, SMK Negeri 1 Ampek Angkek was selected as the research site, and it is an excellent choice for the study's subject.

Data were gathered through observation, interviews, and document analysis studies. Primary and secondary data sources were used as the data sources for this study. Through interviews, primary data sources are directly gathered from informants or sources that are thought to be knowledgeable and reliable providers of information. the vice principals, instructors, and principals in this instance. Documents, specialized literature, study summaries, and other relevant textual materials serve as secondary data sources. Since the problem or aim of this research is connected to the network found within the SMK Negeri 1 Ampek Angkek school, data collecting and analysis are activities that are carried out concurrently. The data acquired will be immediately examined using the qualitative descriptive analysis approach. The organization of the material in the form of pictures, photos, papers, reports, manuals, and other formats is the first stage in this investigation.

## **Results and Discussion**

### **Analyze the Network System**

System analysis is a stage that seeks to comprehend the network system in order to identify its flaws and be able to ascertain its requirements by scrutinizing the current network system's operating procedures. As a result, the current network system can be assessed so that a proposal for a new network system can be made. from the evaluation's findings, including the tools and operating system employed, as well as the security system. Network security using a VPN (Virtual Private Network) using the PPTP (Point To Point Tunneling Protocol) approach at the Kertaraharja Ciamis Village Office is one relevant study, according to a piece by Dewi.S (2020). The configuration of the Virtual Private Network (VPN) Network Design and Implementation using Mikrotik Base, configuration on numerous ethernets, and Winbox

login using a public IP address were the first steps in the research. Then, begin setting Winbox, working your way up to VPN configuration from IP address configuration. The findings of the network security evaluation demonstrate that activity on the VPN network is superior since those actions are not visible to others.

So that security and network activity are improved, this security system may also be used to the school network at SMK Negeri 1 Ampek Angkek. In their research on VPN security, Kumajas, et al. (2022) test the effectiveness of hotspot attacks using wireless usernames and passwords that they break at various ranges while looking for connection sessions. According to tests done with the aircrack program, it cannot solve the wireless username or determine the IP address of the original wireless user; it can only track the configuration of a hotspot's presence. In order to better align educational services at SMK Negeri 1 Ampek Angkek with the fast development of information technology, network analysis will be used (Aripin & Ramdhani, 2021). so that SMK Negeri 1 Ampek Angkek's network security may be better maintained.

### The Operating System of SMK Negeri 1 Ampek Angkek

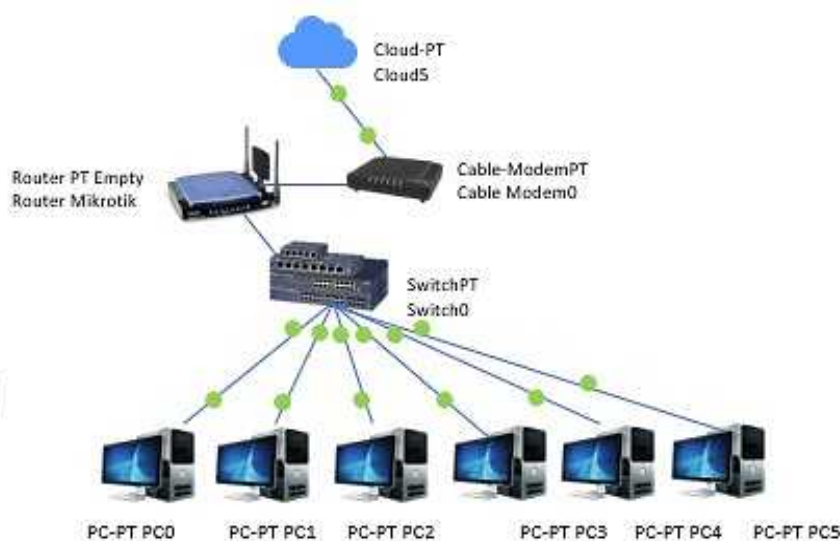


**Figure 1. System of Operation**

Based on the system operating at the SMK Negeri 1 Ampek Angkek computer lab, it is evident that the lab's computer network is connected to the internet, then wirelessly connected to a hub, and then sent to the school lab via a wired network for usage in the space. The network security mechanism is still highly weak because it is well known that computer users in the room no longer require passwords to access to the internet because all users may do so instantly.

### Recommended System

In the analysis that is being proposed, internet packets are distributed to a modem, which then connects the network to a router, which serves as a hotspot, DHCP server, and VPN server. The router is then connected to a switch, which in turn connects all of the local computers to a computer network that will be integrated with database servers. A switch is a component that connects many computers and allows data packets to be distributed among them in a network so that they can travel straight to their intended destination (Sulaiman, 2016).



**Figure 2. Recommended System**

According to the image above, SMK Negeri 1 Ampek Angkek offers wireless network connectivity for Internet use. By connecting a computer or laptop, data will be immediately connected to the user controller PC for management of all operating systems. The hotspot application and VPN (Virtual Private Network) are included as tools in safeguarding the current network. The system the author suggests uses Mikrotik and PVN (Private Virtual Network) to examine computer network security and is beneficial for enhancing network security at SMK Negeri 1 Ampek Angkek. It also includes the addition of hardware devices such routers, modems, and Mikrotik. The application and design of the Mikrotik router's access security from attacks seeks to examine the router's access security system and implement mitigation or preventive measures as well as security solutions from exploit attacks (Raharjo & Iswahyudi, 2021).

Where the server is a computer system that offers specific sorts of services in a computer network, the difference between before and after utilizing the server is that. A scalable CPU, plenty of RAM, and a network operating system all support the server. To put it simply, the server does tasks as requested by a client. For instance, when you use a browser to input a website URL into a web server, your computer is functioning as a client and asking the server for information.

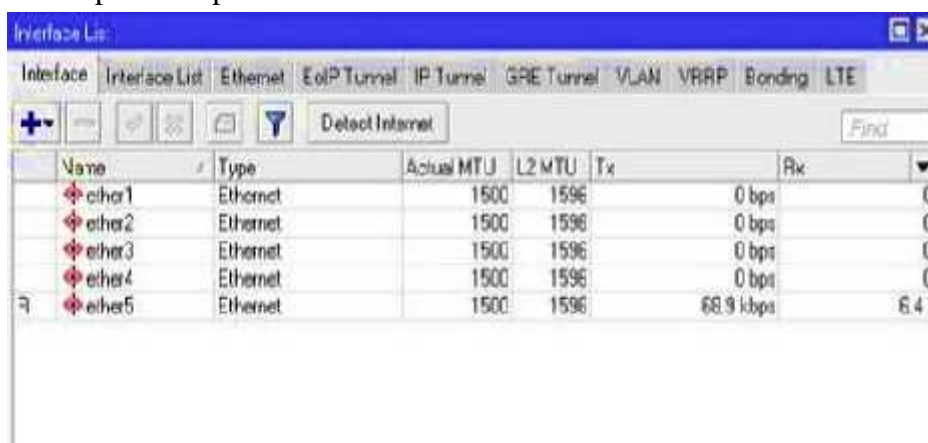
Accessing data on the network demonstrates the outcomes of a network security investigation that used a Virtual Private Network to enhance network security. A device in the form of a proxy is used to enhance the network security system of SMK Negeri 1 Ampek Angkek in order to examine the security system utilizing a VPN. The following steps were taken in order to analyze the network :

**a) Configuration of Mikrotik**

An operating system and piece of software called Mikrotik is used to turn a computer into a router (Gunawan.dkk., 2018). A winbox gadget may be used to connect to Mikrotik. The reason this device is the most common is that in addition to being simple, it can also use a GUI to show menus on the proxy (Graphic User Interface). Winbox is able to identify the MAC address of the installed ethernet 37 on the proxy. After successfully gaining access to the proxy, the first action to take is to name each ethernet interface.

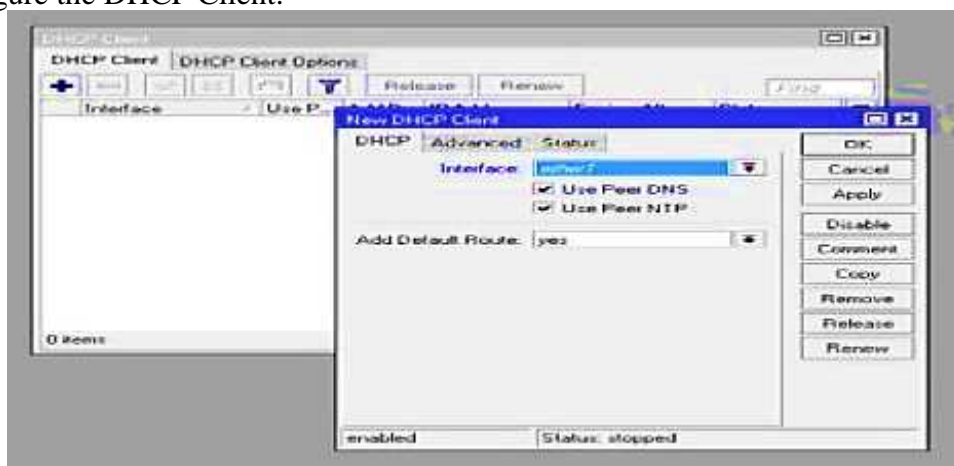
To facilitate configuration, the first step is to provide an identity to each connection on the proxy. Three sections make up the LAN wire attached to the proxy, including: Ether 1: The cable that attaches to the modem for the internet. Ether 2: Local network cable linked. Ether 3: Cable connected to the access point.

Open the interface menu as shown below to give identity : Click Interface > ether1 > Apply > OK to complete the process.



**Figure 3. Interface List**

The following step is to set up the DHCP Client. The purpose of this function is to connect or integrate network connections from the modem to all network clients. Select IP > DHCP Client > (+) > on the interface, select ether1- internet as the network source > Apply > OK to configure the DHCP Client.



**Figure 4. DHCP Client**

The DNS setup seeks to identify the domain name server since the internet network utilizes IP addresses to connect. The author chooses either DNS server 8.8.8.8 or 8.8.4.4 to provide DNS. This DNS seeks to transform the IP address into a domain or name that will facilitate domain search (Bachtiar, 2022). The purpose of an IP Address is to control the addressing of each client so that no clients interfere with one another by assigning an IP Address to identify any ether running on its relevant network class. On switched networks, Internet Protocol (IP) is intended to connect computer communication systems by serving as a network identity address (Dwiyatno,dkk. 2019). The most significant protocol in the Internet Layer is TCP / IP, which is at its core known as Internet Protocol (IP). IP offers packet transportation services on the TCP / IP network that was created (Dewi, 2020).

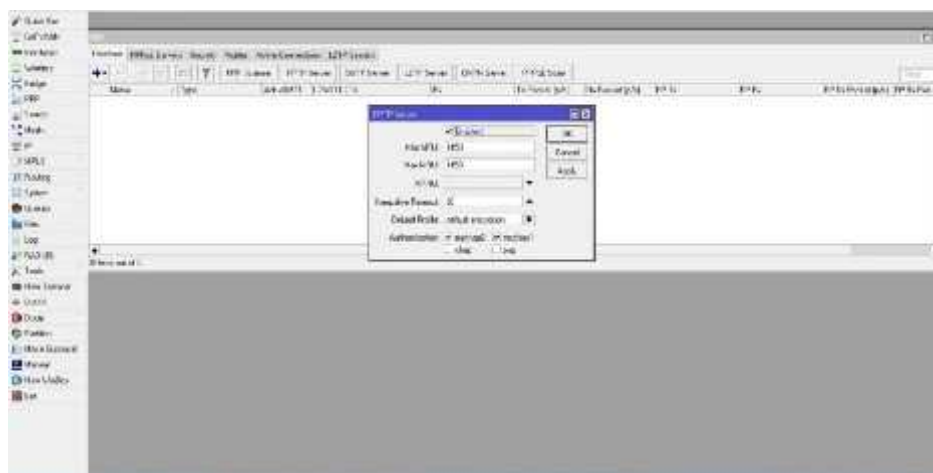


Network interruption is inevitable due to a variety of disruptions, including viruses that spread via the network, heavy traffic-generating activities, and other potential issues. By setting up a firewall to block suspected network activity or interfering with a network that can interfere with network activity, the issue might be resolved. To prevent people from accessing particular material, this step is conducted (Alfred & Chandra, 2018). A computer network is a grouping of computers and other linked devices that enables network users to exchange data among themselves using network-connected hardware and software (Ariyadi & Maulana, 2021).

In order to safeguard client data in the network and to ensure data security when clients interact with one another within the system, a client user and password must be created. The DHCP server configuration comes next, which involves giving the server an IP address so that it can automatically find an IP client. Client computers that are connected to the network ask DHCP servers, which contain a supply of computer IP addresses in their database, for IP addresses (Miftah, 2018).

### b) Configuration of a VPN

After that, set the Mikrotik Router as a VPN server by configuring PPTP on the Mikrotik router. VPN is a private virtual connection since the network generated is not physically visible, it is merely a virtual network, and only certain people may access it, making it private (Oktivasari & Utomo, 2016).



**Figure 5. PPT Server Configuration**

PPT Server Configuration is the process of turning on the VPN server. By selecting PPP->interface->PPTP server from the PPP menu. To encrypt the VPN route, use the "Default-encryption" profile. Then press OK. Furthermore, the establishment of a client user and password is crucial. 1 is a system for securing client data in the network and for securing data when clients interact with one another in the system. The routes gateway is configured by assigning an IP address to the server so that it may connect. Then, on Windows, configure the system. This setting is done by going to the Network and Sharing Center menu, then selecting Set up new connection or network to make a new connection. Select Connect to a workplace in the following box, then click Next. Then choose Use My Internet Connection (VPN), then set up an internet connection before proceeding, and last choose Bradband (PPPoE).



**Figure 6. Broadband (PPPoE)**

By incorporating VPN security into the system, a VPN (Virtual Private Network), a technique for creating a new network within an existing network to increase security, will be configured. An operating system called Network (network) consists of several computers and other network devices that collaborate to accomplish a task (Masse & Iyan, 2016). Clients that have access to data that is often only permitted in specific locations can also use VPN. In this instance, PPTP is used to build the VPN on a network that has traveled via a multi-hop router or the internet.

The author can view a comparison between the pre- and post-study settings after examining the network he or she has built. With a VPN server, it is possible to access student, teacher, staff, and learning data from anywhere as long as there is an internet connection. Currently, a PPTP server may be used to access student, teacher, staff, and learning data from anywhere. Because the actions carried out in VPN tunnels are secret, evaluation of VPN and Non-VPN networks demonstrates that activities on VPN networks are superior than Non-VPNs (Ratmoko & Nurhadiyono, 2012). As a result, individuals may find it simpler to finish their daily schedule.

### **Conclusion**

Several conclusions may be derived from the Virtual Private Network (VPN) network security system's findings. For example, utilizing a VPN at SMK Negeri 1 Ampek Angkek revealed that the access server to the website is safe from intrusions. All data accessible at SMK Negeri 1 Ampek Angkek can be encrypted before being transferred, protecting the contents from being read by careless parties. This includes input values in the network and school privacy data. The Virtual Private Network, which has been implemented at SMK Negeri 1 Ampek Angkek, can be used to restrict client access to information that is often only permitted in specific locations. With a number of Mikrotik capabilities, the deployment of a virtual private network at SMK Negeri 1 Ampek Angkek may also be established for a more secure network. In terms of data interchange via open channels common in schools, the VPN implemented at SMK Negeri 1 Ampek Angkek is a secure option. It seems as though there is no activity on the network at SMK Negeri 1 Ampek Angkek because data that is transferred



over the VPN channel cannot be noticed. Because there is no cap on the amount of data that can be communicated, using a VPN at SMK Negeri 1 Ampek Angkek would make transmitting data at school more convenient while also saving time and money.

### Recommendation

The recommendation made based on the research is that labs and schools should add computers (clients), and that you should be aware of the bandwidth available. Make sure there is a network in the space that can access the internet before creating an internet network with a proxy as the server. In order to prevent data leakage while sharing information over public channels, it is advised to convert to employing VPN technology instead of the manual way that has been used up until now.

### References

- Aripin, N., & Ramdhani, Y. (2021). Implementasi Jaringan Wireless Berbasis Router Mikrotik Dengan Menggunakan Vlan Di Smk Mvp Ars Internasional Bandung. *Eprosiding Teknik Informatika (Protektif)*, 2(1), 97-102.
- Ariyadi, T., & Maulana, A. T. (2021). Penerapan Web Proxy Dan Management Bandwidth Menggunakan Mikrotik Routerboard Pada Kantor Pos Palembang 30000. *Jurnal Ilmiah Informatika*, 9(02), 116-122.
- Bahtiar, D. (2022). Pengenalan Dasar Instalasi Jaringan Komputer Menggunakan Mikrotik. *Jatimika: Jurnal Kreativitas Mahasiswa Informatika*, 2(3).
- Dewi, S. (2020). Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis. *EVOLUSI: Jurnal Sains dan Manajemen*, 8(1).
- Dwiyatno, S., Sulistiyono, S., & Nugraheni, M. (2019). Layanan Komunikasi Voip Menggunakan Raspberry Pi Dan Raspbx Pada Smk Al-Insan Terpadu. *Prosisko: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, 6(2).
- Ekawati, I., & Irwan, D. (2021). Implementasi Virtual Private Network Menggunakan PPTP Berbasis Mikrotik. *JREC (Journal of Electrical and Electronics)*, 9(1), 41-48.
- Gunawan, H., Simorangkir, H., Ghiffari, M., Informatika, T., Komputer, F. I., & Unggul, U. E. (2018). Pengelolaan Jaringan Dengan Router Mikrotik Untuk Meningkatkan Efektifitas Penggunaan Bandwith Internet (Studi Kasus Smk Ki Hajar Dewantoro Kota Tangerang). *Ilmu Komput*, 3(1), 54-70.
- Kumajas, S., Sasukul, J., Siwi, A., & Saruan, H. (2022). Wireless Local Area Network Security through Protocol Wireless Protected Access. *International Journal of Information Technology and Education*, 1(2), 60-71.
- Mananggell, A. V., Mewengkang, A., & Djamen, A. C. (2021). Perancangan Jaringan Komputer Di Smk Menggunakan Cisco Packet Tracer. *Edutik: Jurnal Pendidikan Teknologi Informasi Dan Komunikasi*, 1(2), 119-131.
- Masse, B. A., & Iyan, I. (2016). Membangun Jaringan Wireless Dengan Pengaturan Bandwidth Menggunakan Mikrotik RB951 Pada SMK Negeri 6 Palu. *Jurnal Elektronik Sistem Informasi dan Komputer*, 2(2), 19-28.
- Miftah, Zaeni. (2018). Simulasi Keamanan Jaringan Dengan Metode Dhcp Snooping Dan Vlan. *Faktor Exacta*. 11. 167. 10.30998/Faktorexacta.V11i2.2456
- Moleong, Lexy. J. (2011). *Metode Penelitian Kualitatif*. Bandung: Remaja Rosdakarya
- Mujiastuti, R., & Prasetyo, I. (2021). Membangun Sistem Keamanan Jaringan Berbasis Vpn Yang Terintegrasi Dengan Dns Filtering Pihole. *Prosiding Semnastek*.





- Musdalifa, M., & Panu, S. A. (2019). Perancangan Jaringan Wifi Dengan Menggunakan Mikrotik Pada SMP Negeri 3 Mallusetasi Kabupaten Barru. *Publikasi Pendidikan*, 9(1), 28-41.
- Noviansyah, M., & Saiyar, H. (2021). Pencegahan Packet Sniffing Menggunakan Metode Vpn Tunnel Untuk Keamanan Jaringan Komputer Berbasis Mikrotik. *Jurnal Akrah Juara*, 6(4), 36-46.
- Oktivasari, P., & Utomo, A. B. (2016). Analysis Of Virtual Private Network Using Openvpn And Point To Point Tunneling Protocol-Analisa Virtual Private Network Menggunakan Openvpn Dan Point To Point Tunneling Protocol. *Jurnal Penelitian Komunikasi Dan Opini Publik*, 20(2).
- Putra, J. L., Indriyani, L., & Angraini, Y. (2018). Penerapan sistem keamanan jaringan menggunakan VPN dengan metode PPTP pada pt. asri pancawarna. *IJCIT (Indonesian Journal on Computer and Information Technology)*, 3(2).
- Raharjo, S., & Iswahyudi, C. (2021). Analisis Keamanan Jaringan Mikrotik Isp Indonesia Menggunakan Search Engine Scada Shodan Dengan Metode Exploit Winbox Critical Vulnerability. *Jurnal Jarkom*, 9(1), 56-62.
- Ratmoko, H., & Nurhadiyono, B. (2012). Analisis Implementasi Keamanan Jaringan Virtual Private Network (Vpn) Pada Pt. Layar Sentosa Shipping Corporation. *Jurnal*, 2(1).
- Sulaiman, O. K. (2016). Analisis Sistem Keamanan Jaringan Dengan Menggunakan Switch Port Security. *Cess (Journal Of Computer Engineering, System And Science)* 1(1) 9-14