e-ISSN
JURNAL KOMPUTER

Implementation Of Open Source Security Information Management (OSSIM) On Security Computer Network

Penerapan Open Source Security Information Management (OSSIM) Pada Keamanan Jaringan Komputer

Angga Ardian Putra [1)], Sapri[2)], Abdussalam Al Akbar [3)]
[1,2,3)] ***Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu***
Email: [1)] anggaardianputra18010103@gmail.com

ARTICLE HISTORY
Received [1 November 2022]
Revised [27 November 2022]
Accepted [12 Desember 2022]]

KEYWORDS
Computer Networking, Monitoring, Security

ABSTRAK

Penelitian ini berjudul PENERAPAN Open Source Security Information Management (OSSIM) Pada Keamanan Jaringan Komputer. Yang bertujuan membangun suatu sistem yang dapat melakukan monitoring dan keamanan jaringan komputer di SMA Negeri 1 Seluma. Dimana dalam melakukan monitoring dan kemanan jaringan digunakan sistem Open Source Security Information Management (OSSIM) yang memanfaatkan kibana dan keamanan menggunakan Squert dengan menggunakan sistem operasi linux ubuntu server 20.04. Dalam melakukan monitoring jaringan kibana dapat melakukan monitoring terhadap aktifitas jaringan komputer dengan baik diantaranya memonitoring kegiatan berdasarkan service yang digunakan, dari hasil monitoring tersebut yang mana jika terdapat kegiatan yang tidak di bolehkan seperti membuka situs judi dan lainnya akan dilakukan pengamanan atau pemblokiran dari squert. Secara keseluruhan sistem monitoring dan kemanan berjalan dengan baik. Sistem operasi linux ubuntu server 20.04 sangat baik dalam menjalankan kibana dan squert untuk melakukan monitoring dan keamanan jaringan komputer pada SMA N 1 Seluma.

ABSTRACT

This research is entitled APPLICATION OF Open Source Security Information Management (OSSIM) in Computer Network Security. Which aims to build a system that can monitor and monitor computer network security at SMA Negeri 1 Seluma. Where in monitoring and network security an Open Source Security Information Management (OSSIM) system is used which utilizes kibana and security uses Squert using the Linux Ubuntu Server 20.04 operating system. In monitoring the network, Kibana can monitor computer network activities properly including monitoring activities based on the service used, from the results of this monitoring which if there are activities that are not allowed such as opening gambling sites and others, security or blocking of squert will be carried out. Overall the monitoring and security system is running well. Linux operating system ubuntu server 20.04 is very good at running kibana and squert to monitor and monitor computer network security at SMA N 1 Seluma.

PENDAHULUAN

Perkembangan teknologi jaringan komputer sangat pesat pada era sekarang ini. Banyak orang maupun institusi telah menerapkan sistem informasi yang tidak lepas dari jaringan komputer baik itu intranet maupun internet. Semakin hari pula disiplin ilmu dibidangini semakin beragam

sesuai dengan kebutuhan perkembangan ilmu itu sendiri. Demikian juga ancaman keamanan sistem jaringan juga berjalan seiring perkembangannya.

Dalam sistem jaringan banyak ditemui kekurangan-kekurangan yang sering muncul, diantaranya adalah gangguan berupa virus atau jaringan komputer yang bermasalah dan gangguan dari luar bisa berupa semua bentuk attacking network system. Gangguan sistem jaringan dari dalam bisa saja karena ada otoritas yang menghendaki perbaikan sistem ataupun pengolahan data sistem sehingga meninggalkan gangguan berupa virus ataupun koneksi yang down.

SMA N 1 Seluma merupakan salah satu sekolah kejuruan yang ada di Kabupaten Seluma dan merupakan salah satu sekolah kejuruan yang menjadi pioneer dalam jurusan Teknik Komputer dan Jaringan. Saat ini SMAN 1 Seluma sudah memiliki 1 laboratoium komputer yang memiliki 32 unit komputer.

Saat ini Jaringan komputer yang ada pada SMA N 1 Seluma sudah ada dan berjalan sesuai dengan kebutuhan guna menunjang kegiatan belajar dan mengajar. Untuk pengamanan jaringan saat ini masih bersifat personal pada masing-masing komputer serta belum memiliki sistem monitoring dan keamanan jaringan yang bersifat keseluruhan, sehingga saat ini sering terjadi kesalahan dalam jaringan baik itu berupa jaringan down, performa jaringan, virus (seringnya komputer yang terhubung ke jaringan terinfeksi virus trojan), situs masih bebas dibuka siswa/i, dan masih banyak masalah lainnya.

Dalam melakukan monitoring dan keamanan jaringan banyak tool yang dapat digunakan seperti PRTG Network, OSSIM (Open Source Security Information Management), Nagios dan lainnya begitu juga halnya untuk keamanan jaringan seperti IDS (Instruction Detection System) untuk mendeteksi DOS attack, CGI attack, SQL injection dan lainnya. Akan tetapi untuk dapat melakukan monitoring sekaligus keamanan jaringan yang berjalan sekaligus, salah satunya yaitu OSSIM (Open Source Security Information Management) yang dapat berkerja secara bersamaan dalam melakukan monitoring dan keamanan jaringan. OSSIM (Open Source Security Information Management) adalah distribusi Linux sumber terbuka dan gratis yang dapat melakukan monitoring dan keamanan jaringan.

LANDASAN TEORI

Analisa

Menurut Jefri (2018:82) analisa adalah teknik pemecahan masalah dengan memecah suatu sistem menjadi komponen-komponennya dengan tujuan memahami bagaimana komponen-komponen tersebut bekerja dan berinteraksi untuk mencapai tujuannya. Perancangan sistem merupakan pelengkap dari analisis sistem dalam suatu sistem yang lengkap dengan tujuan untuk mencapai sistem yang lebih baik.

Menurut Yoder (2017: 18) analisa diartikan sebagai prosedur melalui data yang relevan dengan setiap pengamatan dan dicatat secara sistematis.

Sedangkan menurut Kristanto (2019:8) analisa system adalah teknik pemecahan masalah dengan memecah sistem menjadi komponen-komponen dengan tujuan memahami bagaimana komponen-komponen itu bekerja dan berinteraksi untuk mencapai tujuannya. Perancangan sistem merupakan pelengkap dari analisis sistem dalam suatu sistem yang lengkap dengan tujuan untuk mencapai sistem yang lebih baik..

Jaringan Komputer (Computer Network)

Menurut Fahlepi (2018:88) Jaringan komputer adalah kumpulan komputer dan perangkat lain yang saling berhubungan dan membentuk satu kesatuan sistem. Jaringan komputer memungkinkan informasi dan data untuk berpindah dari satu jaringan ke jaringan lain, sehingga memungkinkan pengguna jaringan komputer untuk bertukar dokumen dan data. Tidak hanya itu, jaringan komputer juga memungkinkan pengguna untuk mencetak ke printer yang sama dan menggunakannya bersama-sama.

Menurut Putu (2019:12) Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan melalui protokol komunikasi melalui media transmisi atau komunikasi sehingga dapat berbagi data, informasi, program, dan berbagi perangkat keras. Seperti printer, hard drive, dll.

Menurut Micro (2019:6) Konsep jaringan komputer lahirpada tahun 1940-an di Amerika dari sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan group riset Harvard University yang dipimpin profesor H. Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yangharus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (p), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan dengan kaidah antrian.

Sistem Monitoring

Menurut Prasetyo (2018:48) Monitoring jaringan adalah bagian dari manajemen jaringan. Yang menjadi dasar dari konsep manajemen jaringan adalah adanya manajer atau perangkat yang melakukan manajemen dan agen atau perangkat yang dikelola.

Menurut Pradikta (2018:A154) Monitor dan Manajemen jaringan adalah kemampuan untuk memantau, mengontrol dan menjadwalkan jaringan komputer dan komponen sistem. Pemantauan jaringan adalah bagian dari manajemen jaringan. Yang paling mendasar dalam konsep manajemen jaringan adalah tentang keberadaan manajer atau perangkat manajemen dan agen atau perangkat manajemen..

Monitoring jaringan merupakan tugas yang sulit dan merupakan tugas yang sangat penting bagi seorang administrator jaringan. Seorang adminstrator jaringan selalu berusaha untuk menjaga kelancaran operasi jaringan. Jika jaringan mengalami penurunan kualitas dalam jangka waktu yang singkat saja akan menyebabkan penurunan produktivitas dalam sebuah perusahaan. Dalam hal monitoring jaringan dituntut agar bersifat proaktif daripada reaktif, administator perlu memonitor lalu lintas dan kinerja dari jaringan dan memastikan tidak terjadi pelanggaran keamanan dalam jaringan.

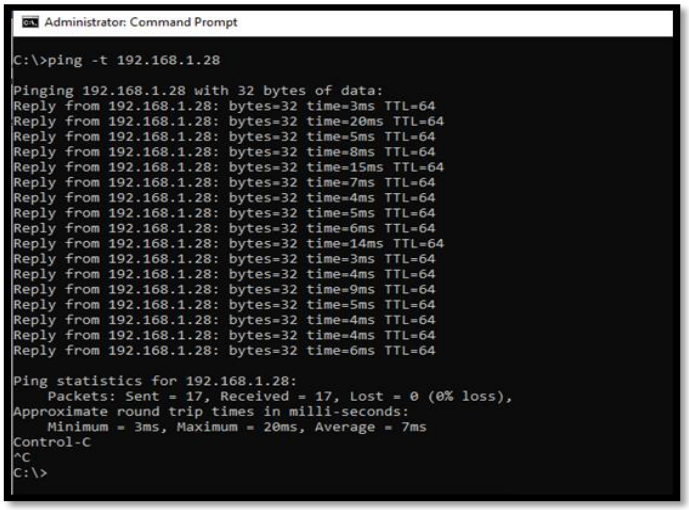
METODE PENELITIAN

Metode penelitian yang digunakan, yaitu penelitian eksperimen. Penelitian dengan pendekatan eksperimen adalah suatu penelitian yang berusaha mencari pengaruh variabel yang lain dalam kondisi yang terkontrol. Metode penelitian yang dilakukan dalam penelitian ini yaitu dengan menggunakan metode eksperimen langsung untuk membangun sebuah sistem monitoring dan keamanan jaringan komputer dengan menggunakan OSSIM pada SMAN 1 Seluma.

HASIL DAN PEMBAHASAN

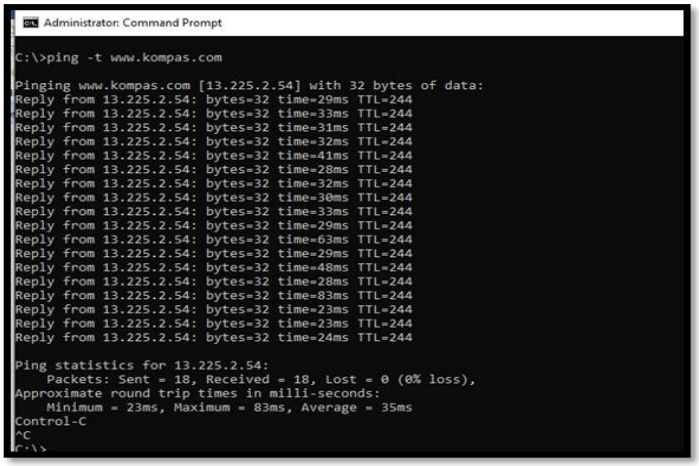
Uji coba dilakukan dengan menguji kemampuan OSSIM dengan menggunakan *tool* Kibana dan Sguil (Squert) dalam melakukan *monitoring* dan keamanan terhadap ancaman Peyebaran, DOS Attack, CGI dan SQL Injeksi pada jaringan komputer pada SMA N 1 Seluma, dimana *tool* pada OSSIM akan melakukan secara bersamaan yang ditampilan pada kibana dan squert dan diamankan oleh sguil. Secara langsung dengan melakukan *monitoring* jaringan komputer pada SMA N 1 Seluma maka secara otomatis akan ikut dalam melakukan peningkatan kualitas jaringan komputer pada SMA N 1 Seluma, Pengujian dilakukan antara lain :

1. Pengujian Koneksi ke Server dan Internet
   Pengujian dilakukan dengan menggunakan Command Prompt windows dengan tujuan untuk memastikan komputer klien sudah terhubung dengan server yaitu dengan melakukan ping dari klien yaitu dengan perintah ping.
   Adapun hasil ping dari klien dapat dilihat pada tampilan gambar dibawah ini :



Gambar 1 Tampilan Penggujian Koneksi Ke Server

Pada pengujian selanjutnya dilakukan pengujian koneksi ke jaringan internet, pada uji coba ini dilakukan ping ke situs www.kompas.com yaitu dengan perintah ping -t www.kompas.com, adapun hasil pengujiannya dapat dilihat pada tampilan gambar dibawah ini :

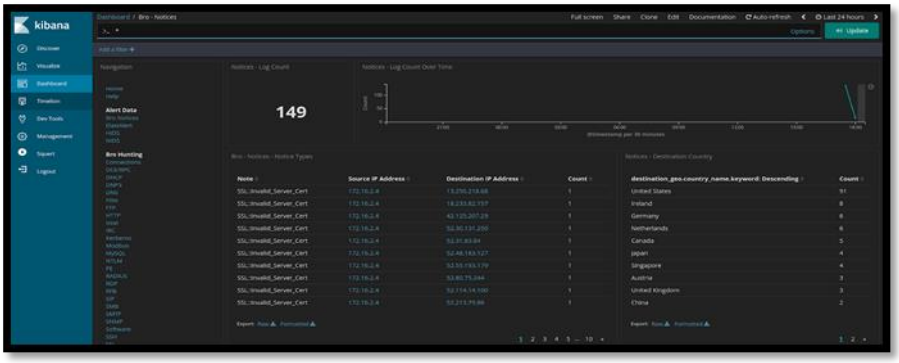


Gambar 2 Tampilan Penggujian Koneksi Ke Internet

Dari tampilan dua gambar diatas dapat dipastikan klien sudah terhubung dengan server OSSIM dan juga internet, yaitu dengan ping reply, jika tidak terhubung maka RTO (*Request Time Out*).

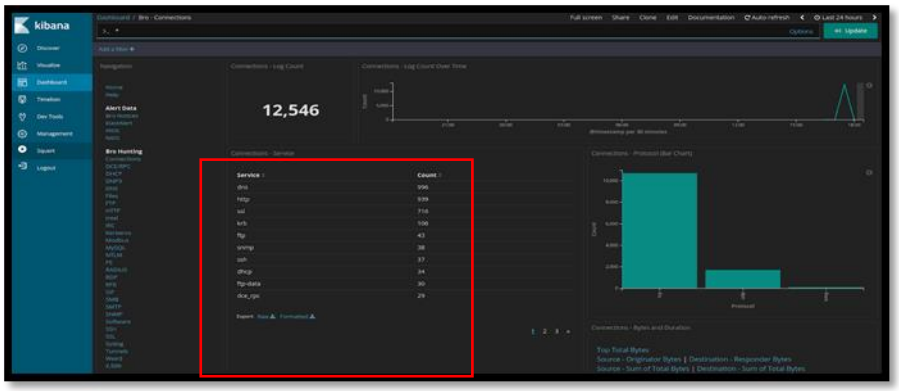
2. *Monitoring* Jaringan Menggunakan Kibana

Pengujian ini dilakukan dengan cara melakukan *monitoring* jaringan menggunakan kibana, adapun tampilan hasil *monitoring* dapat dilihat pada gambar berikut ini :



Gambar 3 Tampilan *Monitoring* Kibana

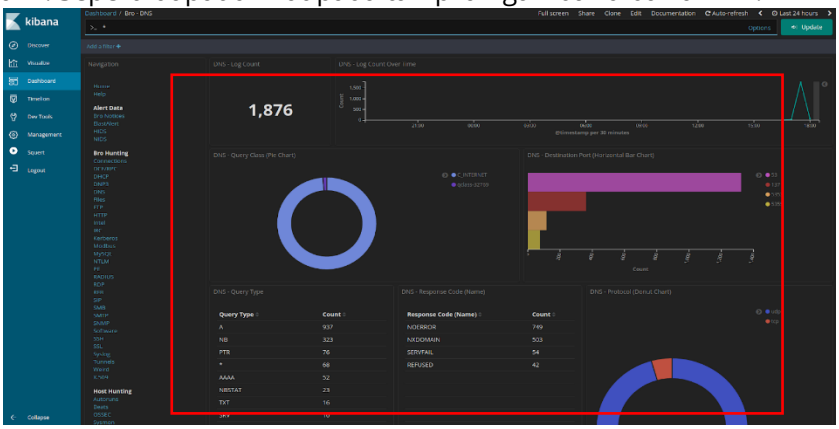
Hasil *monitoring* diatas merupakan tampilan *monitoring* jaringan yang berhasil dilakukan oleh OSSIM dengan menggunakan *tool* kibana. Adapun hasil *monitoring*nya dapat menampilkan ip *address* yang konek kejaringan.



Gambar 4. Tampilan Hasil *Monitoring Service*

Tampilan gambar diatas merupakan hasil *monitoring* jaringan berdasarkan layanan (*service*) server. Dimana kibana dapat melakukan *monitoring* service dan count (kejadian pada *service*).

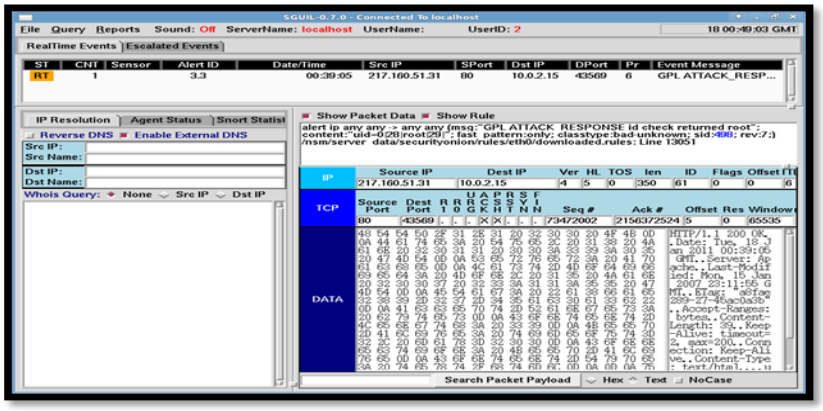
Dan disamping itu kibana juga dapat menampilkan data hasil *monitoring* jaringan komputer dalam bentuk grafik. Seperti dapat dilihat pada tampilan gambar dibawah ini :



Gambar 5 Tampilan Hasil *Monitoring* Dalam Bentuk Grafik

3. Keamanan Jaringan Menggunakan Sguil

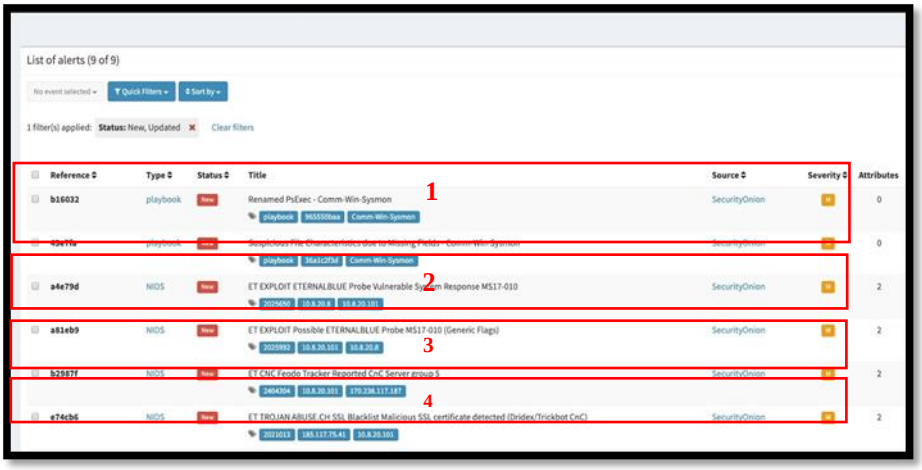
Pengujian ini dilakukan dengan cara melakukan keamanan jaringan menggunakan Sguil, adapun tampilan hasil keamanan dapat dilihat pada gambar berikut ini :



Gambar 6 Tampilan Hasil Kemanan Sguil

Hasil keamanan jaringan komputer diatas OSSIM dengan *tool* Sguil dapat melakukan pengaman jaringan dari ancaman malware attack dengan menggunakan teknik manipulasi time, hal ini dapat dilihat dari report pada bagian data (gambar diatas).

Adapun hasil *monitoring* dan keamanan jaringan komputer dengan menggunakan OSSIM dapat ditampilkan secara detail pada Sguil. Seperti dapat dilihat pada tampilan gambar dibawah ini



Gambar 7 Tampilan Ancaman Yang Berhasil Diamankan

Dari tampilan gambar diatas sistem operasi OSSIM dengan menggunakan kibana dan Sguil (Squert) dapat berjalan dengan baik dimana hasil deteksi akan ditampilan pada kibana dan dilakukan pengamanan oleh Sguil (Squert), seperti dapat dilihat pada tampilan gambar diatas yang ditandai dengan kotak merah.

a) OSSIM Melalui kibana dan Sguil (Squert) dapat melakukan deteksi dan pengamanan terhadap ancaman serangan CGI (berusaha melakukan modifikasi pada file sistem).
b) OSSIM Melalui kibana dan Sguil (Squert) berhasil melakukan deteksi dan pengamanan terhadap ancaman berupa SQL Injeksi (Exploid) dengan report "*ET Exploid Eternal Blue……*".
c) OSSIM Melalui kibana dan Sguil (Squert) berhasil melakukan deteksi dan pengamanan jaringan terhadap ancaman (serangan) DOS (ancaman berupa pengiriman paket berulang menggunakan CNC) yang dilakukan menggunakan aplikasi dengan report "*CNC Feodo Tracker…….*"
d) OSSIM Melalui kibana dan Sguil (Squert) berhasil melakukan deteksi dan pengamanan jaringan terhadap ancaman virus (Trojan) dengan report "*ET Trojan Abuse CH SSL……..*"

Dari serangkaian pengujian yang dilakukan maka didapat hasil seperti dapat dilihat pada table dibawha ini:

Tabel 1. Hasil Pengujian

No	Indikator Pengujian	Hasil	Ket
1	Kemampuan Sistem Operasi Linux Ubuntu Server 20.04 dalam menjalan OSSIM	Sistem operasi linux ubuntu server 20.04 baik dalam menjalan Open Source Security Information Management (OSSIM). Tool yang digunakan untuk melakukan monitoring yaitu kibana dan untuk melakukan pemblokiran atau keamanan menggunakan squirt.	Baik
2	Kemampuan OSSIM dalam mengatasi penyebaran virus dalam jaringan computer SMAN 1 Seluma	OSSIM melalui tool squirt dapat melakukan pemblokiran alamat website yang dianggap atau tidak boleh diakses siswa.	Baik
3	Kemampuan OSSIM dalam mengatasi keamanan jaringan komputer SMAN 1 Seluma	Dalam melakukan keamanan jaringan dapat dilakukan berdasar alamat IP Address. Squirt tidak dapat melakukan blokir berdasarkan alamat url web.	Baik
4	Kemampuan OSSIM dalam melakukan Monitoring jaringan computer pada SMA N 1 Seluma, seperti lalu lintas data, trafik, UP/Down	Dalam melakukan monitoring lalu lintas data OSSIM dapat melakukannya melalui tool kibana. Dimana dapat dilakukan monitoring berdasarkan service yang digunakan.	Baik

KESIMPULAN DAN SARAN

Kesimpulan

1. OSSIM sangat baik digunakan dalam melakukan monitoring dan keamanan jaringan komputer, khususnya jaringan komputer pada SMA N 1 Seluma, karena OSSIM memiliki banyak tool yang dapat melakukan monitoring dan keamanan, diantaranya Kibana dan Sguil.
2. Dalam melakukan monitoring jaringan komputer, Kibana dapat melakukan dengan baik dengan hasil monitoring yang mudah di pahami, seperti penggunaan service sebanyak berapa kali (Count) dan juga hasil dapat ditampilkan dalam bentuk grafik.
3. Untuk melakukan keamanan jaringan komputer OSSIM dengan menggunakan tool Sguil dapat bekerja dengan baik yaitu dengan dapat menampilkan ancaman yang ada.

Saran

1. Dalam penelitian ini penulis menyadari banyak kekurangan-kekurangan, sehingga penulis sangat mengharapkan masukan dan kritikan dan semua pihak agar penelitian ini jadi lebih bermanfaat kedepannya.
2. Untuk penelitian yang akan datang, sistem monitoring dan keamanan jaringan ini dapat dikembangkan dengan menambahkan tool manajemen jaringan.

DAFTAR PUSTAKA

Dwi Bayu Rendro. 2020. Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software NMAP (Studi Kasus Di SMK NEGERI 1 Kota Serang). Jurnal PROSISKO. Rekayasa Sistem Komputer, Fakultas Teknologi Informasi, Universitas Serang Raya

Fahlepi Roma Doni. 2018. Jaringan Komputer dengan Router Mikrotik. Simposium Nasional Ilmu Pengetahuan dan Teknologi (SIMNASIPTEK). Program Studi Teknik Informatika AMIK Bina Sarana Informatika Purwokerto

Jefri Nugraha. 2018. Analisa Dan Perancangan Sistem Informasi Erpustakaan. Jurnal SIMETRIS. Program Studi Sistem Informasi Universitas Muria Kudus
Kristanto. 2019. Analisa, Kuantitas dan Harga – Edisi Revisi. Graha Ilmu. Yogyakarta
Micro, Andi. 2019. Dasar-dasar Jaringan Komputer. Madcom. Palembang
Prasetyo. 2018: Teknik-teknik Pemantau Jaringan Skala Lokal. PT. Elek Media Coputindo. Jakarta
Pratama. Pratama I. 2019. Handbook. Jaringan komputer Edisi Revisi – Jilid ke 2. Informatika. Bandung
Sofana, Iwan. 2017. Cisco CCNA & Jaringan Komputer. Bandung:Informatika Bandung
Sukaridhoto, Sritrusta. 2019. Jaringan Komputer. Informatika. Bandung
Sukaridhoto, Sritrusta. 2019. Komunikasi Data & Komputer - Dasar-Dasar Komunikasi Data. Informatika. Bandung
Yoder. 2017. Analisis dan desain, Sistem Informasi: Pendekatan terstruktur Teori dan Praktek Aplikasi Bisnis, Yogjakarta: Andi Offset.