Jurnal Ilmu Komputer dan Sistem Informasi (JIKSI)

Vol. 11, No. 8, Agustus 2025, hlm. 6-18

IMPLEMENTASI KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN OPEN SOURCE SECURITY INFORMATION MANAGEMENT (OSSIM) PADA SMAN 11 LUWU

Revi Firdayanti Risa[1], Siaulhak[2], Jumarniati[3]
revifirdayantirisa@gmail.com[1], siaulhak@uncp.ac.id[2], jumarniati@uncp.ac.id[3]
Universitas Cokroaminoto Palopo

Abstrak

Penelitian ini bertujuan untuk mengetahui hasil implementasi keamanan jaringan komputer menggunakan Open Source Security Information Management (OSSIM) pada SMAN 11 Luwu. Berawal dari permasalahan yang ada bahwa sekolah ini belum memiliki sistem keamanan yang memadai untuk memantau jaringan komputer. Sekolah ini memiliki jaringan internet yang dimana jaringan tersebut rentan terhadap serangan jaringan, karena sekolah belum menerapkan sebuah sistem keamanan jaringan yang kuat. Penelitian ini dilakukan untuk mendeteksi jaringan dari serangan dengan menerapkan keamanan system monitoring jaringan komputer menggunakan open source security information management. Penelitian ini menggunakan metode action research untuk memonitoring keamanan jaringan serta mendeteksi ancaman. Implementasi Ossim bertujuan mendeteksi ancaman jaringan secara real-time. Hasil penelitian menunjukkan bahwa OSSIM dengan dashboard kibana dan sguil mampu memonitoring dan menampilkan hasil keamanan serta mengamankan ancaman yang ada dengan bantuan tool keamanan seperti snort.

Kata Kunci: Implementasi, Keamanan Jaringan, Ossim, Action Research.

1. PENDAHULUAN

Di era modern saat ini, perkembangan teknologi jaringan komputer mengalami kemajuan yang sangat cepat. Baik individu maupun lembaga telah banyak menerapkan sistem informasi yang terintegrasi dengan jaringan komputer, baik dalam bentuk intranet maupun internet. Seiring dengan kemajuan tersebut, cakupan keilmuan dalam bidang jaringan juga semakin meluas, menyesuaikan dengan dinamika kebutuhan informasi teknologi. Namun demikian, seiring dengan pesatnya perkembangan ini, muncul pula berbagai ancaman terhadap keamanan jaringan. Dalam implementasinya, sistem jaringan sering kali mengalami berbagai permasalahan, seperti serangan virus, gangguan koneksi, hingga ancaman eksternal yang dikenal sebagai serangan jaringan. Selain itu, gangguan internal juga dapat terjadi, misalnya akibat kebijakan otoritas yang melakukan pembaruan sistem atau pengelolaan data, yang tanpa disadari dapat meninggalkan celah berupa penurunan kualitas koneksi atau masuknya malware ke dalam sistem (Putra, 2022).

Salah satu dari banyak sistem yang tersedia untuk semua bisnis di seluruh dunia adalah sistem pemantauan jaringan. Di banyak bisnis, sistem pemantauan dapat digunakan untuk tugas-tugas yang sangat penting. Ada beberapa aktivitas yang dilakukan antara jaringan yang dijalankan oleh berbagai bisnis. Kejahatan dunia maya adalah salah satu aktivitas yang dapat terjadi di jaringan, seperti pencurian data atau pencurian kata sandi akun dari server perusahaan. Namun, ini adalah kenyataan yang sering tidak dipertimbangkan oleh banyak bisnis. Setiap bisnis membutuhkan sistem pemantauan untuk jaringannya karena sistem ini melacak kualitas dan pemeliharaan jaringan.

Pemanfaatan Open Source Security Information Management (OSSIM) sebagai

sistem pemantauan jaringan memberikan kemampuan untuk menyajikan informasi terkait keamanan jaringan secara cepat dan akurat, sekaligus mengumpulkan log serta notifikasi yang dihasilkan oleh berbagai perangkat keamanan jaringan. Dengan sistem ini, administrator dapat mengirimkan peringatan melalui email secara otomatis dan memadukan kondisi jaringan secara real-time, selama 24 jam penuh. Hal ini memudahkan setiap administrator untuk memahami dan mengawasi status jaringan kapan saja selama jaringan sedang beroperasi. Dalam kegiatan monitoring serta pengamanan jaringan, tersedia beragam perangkat yang bisa digunakan seperti Paessler Router Traffic Graapher (PRTG) network monitor, nagios, OSSIM, dan sebagainya. Sementara itu, untuk aspek keamanan jaringan, terdapat alat seperti Intrusion Detection System (IDS) yang dapat mendeteksi berbagai serangan seperti serangan Denial Of Service (DOS), serangan Common Gateway Interface (CGI), dan injeksi Structured Query Language (SQL). Namun, untuk solusi yang mampu menjalankan fungsi monitoring sekaligus pengamanan secara bersamaan, OSSIM menjadi salah satu pilihan yang efektif. OSSIM sendiri merupakan distribusi linux berbasis open-source dan tersedia secara gratis, yang dirancang untuk menyatukan sekaligus menjaga keamanan jaringan dalam satu sistem terintegrasi (Putra, 2022).

SMAN 11 Luwu merupakan salah satu sekolah yang ada di luwu, yang belum memiliki sistem keamanan yang memadai untuk memantau jaringan komputer. Sekolah ini memiliki jaringan internet yang dimana jaringan tersebut rentan terhadap serangan jaringan, karena sekolah belum menerapkan sebuah sistem keamanan jaringan yang kuat. Hingga saat ini, belum tersedia sistem keamanan yang mampu melakukan analisis, sehingga serangan masih dapat terjadi dan berisiko menimbulkan dampak serius terhadap server. Maka dari itu, jaringan di sekolah ini bisa saja diretas oleh pihak luar yang dapat mengakses internet secara bebas, yang dapat menimbulkan masalah saat jaringan digunakan.

Dengan demikian, potensi serangan siber atau akses tidak sah menjadi sangat besar, karena tanpa adanya sistem monitoring, sulit untuk mendeteksi dan mencegah tindakan ilegal seperti kebocoran data atau kerusakan pada sistem.

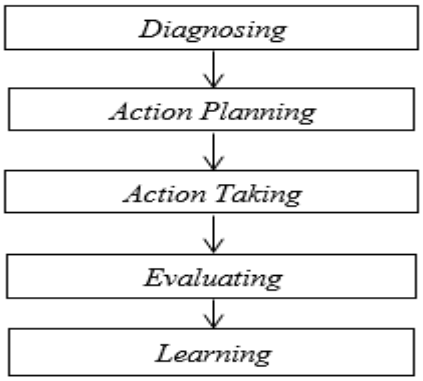
Berdasarkan uraian diatas, melihat permasalahan yang ada pada SMAN 11 Luwu, dapat diatasi dengan mendeteksi jaringan dari serangan dengan menerapkan keamanan system monitoring jaringan komputer menggunakan open source security information management. Hal ini memungkinkan administrator untuk dengan mudah memahami kondisi jaringan kapan saja, selama jaringan komputer digunakan.

Berdasarkan ringkasan diatas, penulis mengambil judul dari penelitian ini sebagai Implementasi keamanan jaringan komputer menggunakan open source security information management (OSSIM). Oleh karena itu, diharapkan penelitian ini dapat memberikan panduan kepada SMAN 11 Luwu.

2. METODE PENELITIAN

Jenis penelitian ini merupakan komponen yang paling penting dalam penelitian. Metode penelitian yang digunakan dalam penelitian ini adalah action research (AR) atau metode penelitian tindakan.

Action research adalah kegiatan atau tindakan perbaikan terhadap sesuatu yang perencanaan, pelaksanaan, dan evaluasinya dilakukan secara sistematis sehingga validitas dan reliabilitasnya sesuai dengan standar penelitian. Adapun siklus action research sebagai berikut:



Gambar 19. Siklus Action Research
Sumber: Hasil Rancangan Penulis (2025)

3. HASIL DAN PEMBAHASAN

Setelah menganalisa masalah yang ada, pada tahap ini yaitu melakukan tindakan terhadap perencanaan dari sistem yang diusulkan pada SMAN 11 Luwu. Tindakan yang akan dilakukan yaitu, mengimplementasikan OSSIM sebagai keamanan jaringan komputer seperti keamanan sistem *monitoring* jaringan pada SMAN 11 Luwu.

1. Perencanaan (*Action Planning*)

Pada tahap perencanaan, penulis melakukan analisis kebutuhan sistem keamanan jaringan yang sesuai untuk diterapkan di lingkungan SMAN 11 Luwu. Perencanaan ini mencakup identifikasi perangkat keras dan perangkat lunak yang dibutuhkan. Penulis mengidentifikasi kebutuhan utama dalam sistem keamanan jaringan di SMAN 11 Luwu, seperti perlunya sistem pemantauan keamanan jaringan. OSSIM (*open source security information management*) dipilih karena merupakan platform *open source* yang mengintegrasikan fitur keamanan.

Penentuan spesifikasi *server* OSSIM dilakukan berdasarkan kebutuhan kapasitas data dan jumlah perangkat yang akan dipantau. Selain itu, dilakukan perancangan letak server OSSIM dalam jaringan sekolah. OSSIM direncanakan akan diintegrasikan dengan sensor keamanan jaringan seperti *dashboard* pemantauan seperti *kibana* dan *sguil* direncanakan untuk membantu memonitoring serta mengamankan jaringan dari ancaman.

Perencanaan ini dilakukan untuk memastikan bahwa implementasi OSSIM dapat berjalan dengan efektif dan efisien dalam meningkatkan keamanan jaringan komputer di SMAN 11 Luwu.

2. Tindakan (*Action Taking*)

Pada tahap ini, penulis melakukan tindakan dengan melakukan implementasi OSSIM.

a. Implementasi OSSIM

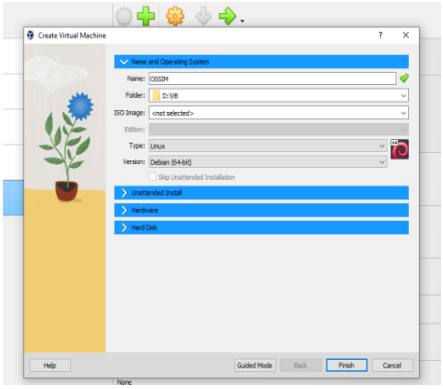
OSSIM diimplementasikan pada SMAN 11 Luwu untuk, mengetahui apakah OSSIM ini mampu memonitoring dan mendeteksi keadaan jaringan komputer.

1) Instalasi *AlienVault*

Langkah pertama yang dilakukan penulis adalah dengan mendownload file ISO *AlienVault* OSSIM pada link (https://archive.org/details/alien-vault-ossim-64bits-4.13.0), kemudian pilih ISO IMAGE pada bagian opsi download:

Gambar 23. Tampilan Download File ISO AlienVault OSSIM
Sumber: Hasil Tangkapan Layar Penulis (2025)

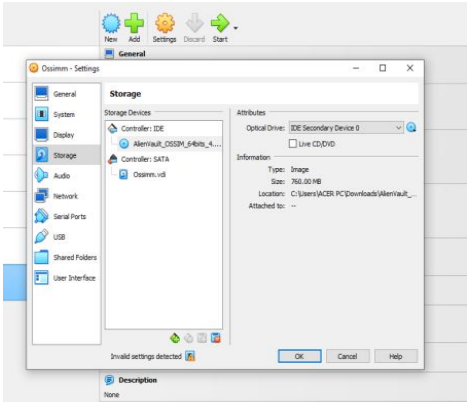
Setelah file ISO didownload, penulis melakukan instalasi *AlienVault* OSSIM pada VM *VirtualBox* dengan cara klik pada icon *New* lalu dibuat seperti tampilan dibawah, lalu klik *Finish*:



Gambar 24. Membuat *Virtual Machine* OSSIM

Sumber: Hasil Tangkapan Layar Penulis (2025)

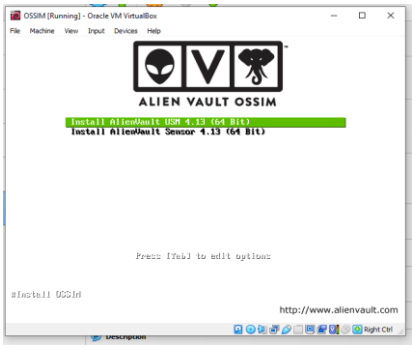
Selanjutnya pada *icon settings*, klik bagian *storage* lalu klik pada bagian *empty* untuk menambahkan file ISO yang sudah didownload lalu tekan ok:



Gambar 25. Menambahkan File ISO

Sumber: Hasil Tangkapan Layar Penulis (2025)

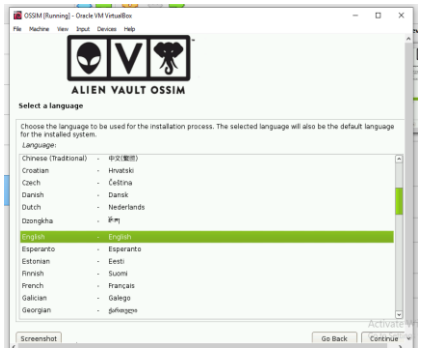
Untuk langkah selanjutnya, penulis menjalankan *virtual machine* yang sudah dibuat, dan akan muncul tampilan menu utama instalasi OSSIM seperti gambar dibawah, pilih *install AlienVault* USM karena itu yang diperlukan untuk instalasi lengkap OSSIM bukan hanya sensor nya saja, lalu tekan enter:



Gambar 26. Menu Utama Instalasi OSSIM

Sumber: Hasil Tangkapan Layar Penulis (2025)

Selanjutnya, pada tampilan pilih bahasa atau *select a language* penulis memilih English, karena merupakan standar bahasa untuk sistem operasi linux dan menghindari bug atau eror tampilan karena bahasa selain english sering tidak didukung penuh oleh sistem. Setelah pilih English, kemudian tekan enter:



Gambar 27. Tampilan Pilihan Bahasa

Sumber: Hasil Tangkapan Layar Penulis (2025)

Selanjutnya pada tampilan *select your location* pilih *other*-asia-indonesia dengan menggunakan tombol panah pada keyboard, *kemudian tekan enter:*

Gambar 28. Tampilan Pilihan Lokasi

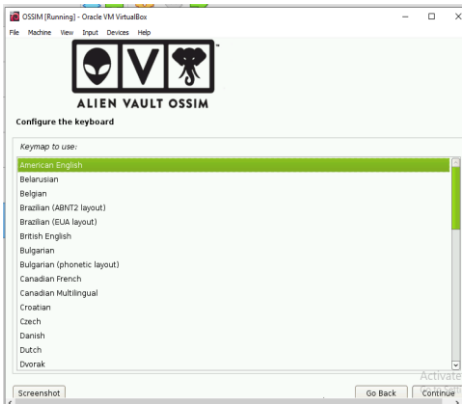
Sumber: Hasil Tangkapan Layar Penulis (2025)

Pada tampilan *configure locales,* penulis memilih *united states* kemudian tekan enter:

Gambar 29. Tampilan Pilihan *Configure Locales*

Sumber: Hasil Tangkapan Layar Penulis (2025)

Pada tampilan *configure the keyboard,* penulis memilih *American English* lalu tekan enter:



Gambar 30. Tampilan Pilihan *Configure Keyboard*

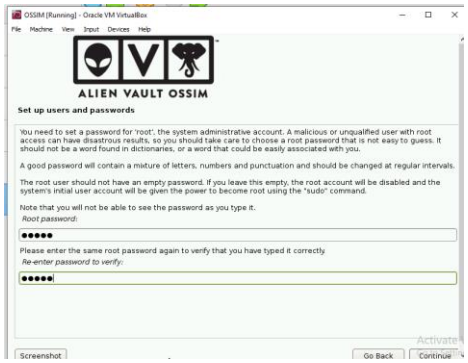
Sumber: Hasil Tangkapan Layar Penulis (2025)

Tampilan selanjutnya yaitu, penulis memasukkan IP yang sudah disesuaikan dengan jaringan sekolah, kemudian tekan enter:

Gambar 31. Tampilan IP *Server*

Sumber: Hasil Tangkapan Layar Penulis (2025)

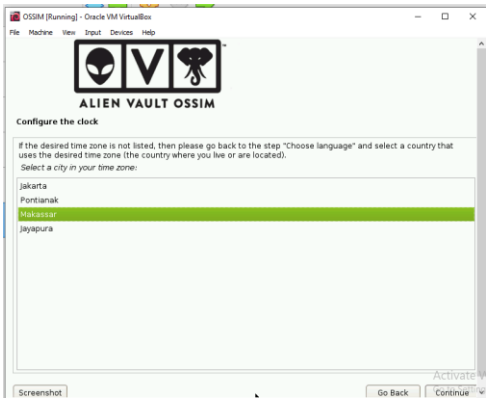
Selanjutnya, penulis membuat *password* untuk login *AlienVault* OSSIM setelah proses instalasi selesai, kemudian tekan enter:



Gambar 32. Tampilan Membuat *Password*

Sumber: Hasil Tangkapan Layar Penulis (2025)

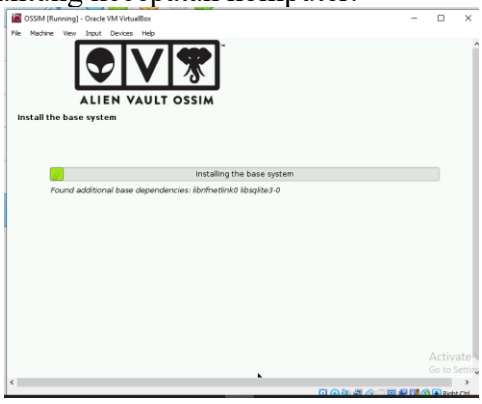
Selanjutnya, zona waktu tersebut dipilih karena waktu Makassar sesuai dengan waktu di daerah penulis yaitu di Luwu, kemudian tekan enter:



Gambar 33. Tampilan Pilihan Waktu

Sumber: Hasil Tangkapan Layar Penulis (2025)

Pada tampilan *install the base system* berikut, tunggu sampai proses selesai dan ini memakan waktu yang lumayan lama atau tergantung kecepatan komputer:

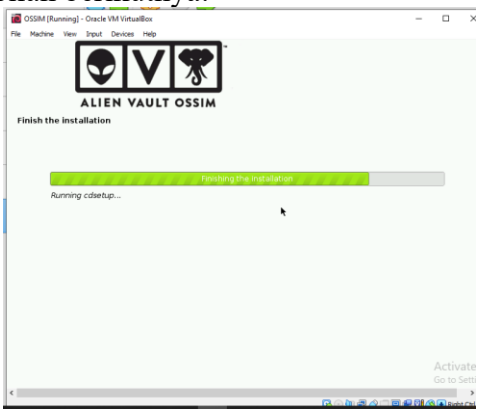


Gambar 34. Tampilan *Install Base System*

Sumber: Hasil Tangkapan Layar Penulis (2025)

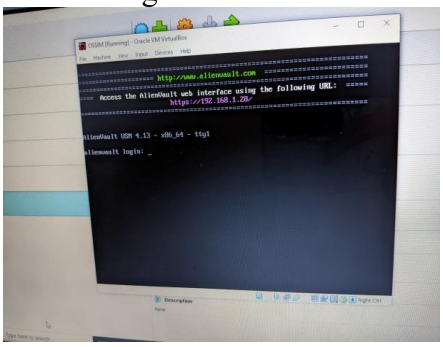
Setelah muncul tampilan *Finish the installation,* artinya proses instalasi OSSIM

sudah selesai, tunggu sampai muncul tampilan berikutnya:



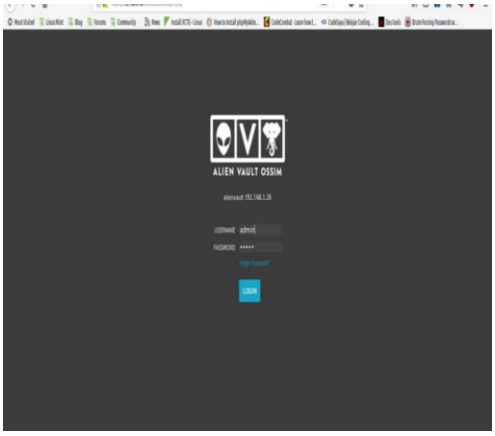
Gambar 35. Tampilan *Finish the Installation*
Sumber: Hasil Tangkapan Layar Penulis (2025)

Setelah penginstalan selesai, berikut tampilan login ke *AlienVault* untuk melakukan konfigurasi:



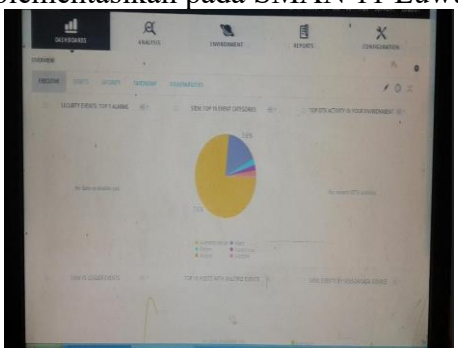
Gambar 36. Tampilan *Login AlienVault*
Sumber: Hasil Tangkapan Layar Penulis (2025)

Selanjutnya login pada server *AlienVault,* mengakses *AlienVault* dengan tampilan *web interface* untuk masuk pada tampilan OSSIM, penulis mengakses melalui *web browser* dengan mengakses (https://192.168.1.28) yang merupakan *ip address* yang sudah disesuaikan dan digunakan untuk mengakses antarmuka web *Alienvault* OSSIM:



Gambar 37. Tampilan *Login AlienVault* OSSIM
Sumber: Hasil Tangkapan Layar Penulis (2025)

Berikut tampilan awal *AlienVault* OSSIM yang berhasil diinstall dan diimplementasikan pada SMAN 11 Luwu:



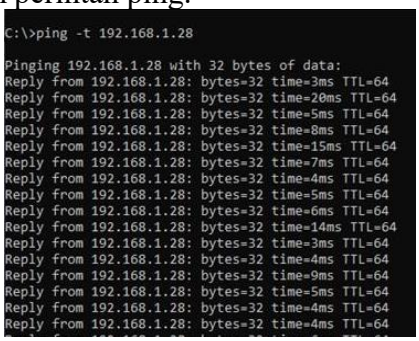
Gambar 38. *Dashboard AlienVault* OSSIM
Sumber: Hasil Tangkapan Layar Penulis (2025)

Uji coba dilakukan dengan menguji kemampuan OSSIM dengan menggunakan *dashboard kibana* dan *sguil* dengan komponen pendukungnya seperti *snort* dalam mendeteksi dan melakukan *monitoring* keamanan terhadap penyebaran ancaman, dimana *tool* pada OSSIM akan melakukan secara bersamaan yang ditampilkan pada *kibana* dan *sguil*. Secara langsung dengan melakukan *monitoring* jaringan komputer pada SMAN 11 Luwu maka secara otomatis akan ikut dalam melakukan peningkatan kualitas jaringan komputer pada SMAN 11 Luwu, Pengujian dilakukan antara lain:

b. Pengujian Koneksi ke *Server* dan Internet

Pengujian dilakukan dengan menggunakan *command prompt windows* dengan tujuan untuk memastikan komputer klien sudah terhubung dengan *server* yaitu

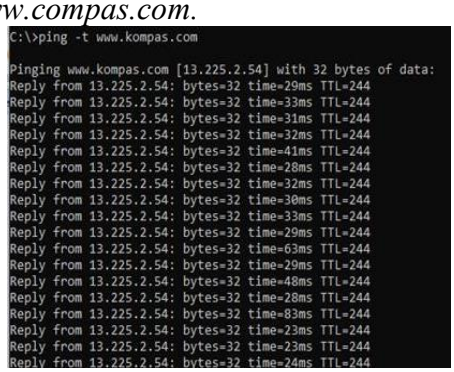
dengan melakukan ping dari *klien* yaitu dengan perintah ping.



Gambar 39. Pengujian Koneksi ke *Server*

Sumber: Hasil Tangkapan Layar Penulis (2025)

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.compas.com*.



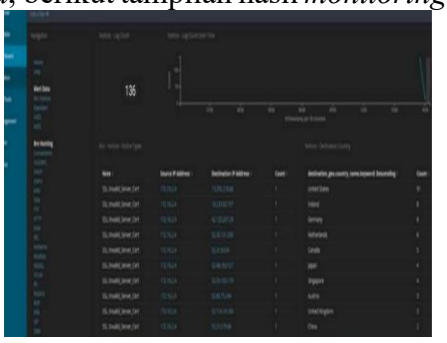
Gambar 40. Pengujian Koneksi ke Internet

Sumber: Hasil Tangkapan Layar Penulis (2025)

Dari tampilan dua gambar diatas, dipastikan *klien* sudah terhubung dengan *server* OSSIM dan juga internet, yaitu dengan *ping reply*, jika tidak terhubung maka RTO (*request time out*).

c. Monitoring Jaringan Menggunakan *Kibana*

Pengujian ini dilakukan dengan cara melakukan *monitoring* jaringan menggunakan *kibana*, berikut tampilan hasil *monitoring:*



Gambar 41. Data *Monitoring Kibana*

Sumber: Hasil Tangkapan Layar Penulis (2025)

Hasil *monitoring* tersebut merupakan tampilan *monitoring* jaringan pada SMAN 11 Luwu yang berhasil dilakukan oleh OSSIM dengan menggunakan *dashboard kibana*. Adapun hasil *monitoring*nya dapat menampilkan *ip address* yang konek ke jaringan.

OSSIM menggunakan *kibana* sebagai antarmuka *monitoring* visual. Hasil pengujian dapat dilihat pada menu *timelion*:

1) *Kibana* menampilkan daftar *IP address* yang terkoneksi
2) Dapat memantau aktivitas *service* jaringan
3) Hasil *monitoring* divisualisasikan dalam bentuk grafik yang mudah dipahami
4) Angka 136 yang merupakan angka deteksi ancaman

Fitur ini membantu *admin* mengetahui lalu lintas data serta identifikasi *service* mana yang sering digunakan.

Gambar 42. Hasil *Monitoring Service*

Sumber: Hasil Tangkapan Layar Penulis (2025)

Tampilan gambar diatas merupakan hasil *monitoring* jaringan berdasarkan layanan (*service*) *server*. Dimana *kibana* dapat melakukan *monitoring service* (pengawasan terhadap status layanan) dan *count* (jumlah kejadian yang tercatat pada kejadian di *service*).

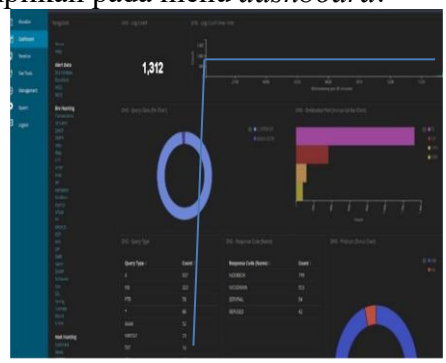
Pada gambar ini terlihat informasi yang ditampilkan pada menu *squert* tentang layanan (*services*) yang sedang berjalan di jaringan sekolah, termasuk:

1) Jenis layanan atau protokol yang

digunakan, seperti http, ftp, dns
2) Jumlah koneksi atau aktivitas (*count*) yang terjadi terhadap layanan tersebut
3) Angka 10,314 yang merupakan jumlah keseluruhan *log* aktivitas yang tercatat

Melalui pemantauan layanan jaringan ini, *administrator* dapat mengetahui layanan apa saja yang aktif atau sering diakses, dan jumlah kejadian yang tercatat pada *service.*

Selain itu, *kibana* juga mampu menyajikan data hasil pemantauan jaringan komputer dalam format grafik yang ditampilkan pada menu *dashboard*:



Gambar 43. Data *Monitoring* dalam Bentu Grafik
Sumber: Hasil Tangkapan Layar Penulis (2025)

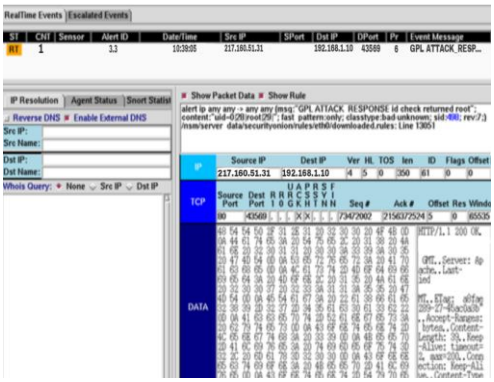
Gambar ini menampilkan visualisasi data *monitoring* jaringan pada SMAN 11 Luwu yang dilakukan menggunakan *kibana* yang dilengkapi dengan komponen pendukung**,** bagian dari OSSIM. Dalam gambar tersebut, data aktivitas jaringan ditampilkan dalam bentuk grafik batang atau *linier*, yang menggambarkan:

1) Jumlah koneksi atau kejadian (*events*) berdasarkan waktu ditampilkan pada garis pojok kanan atas
2) Jenis layanan atau protokol yang digunakan dalam jaringan, yaitu http dan dns ditampilkan pada pojok kanan bawah
3) Volume trafik data atau aktivitas yang terjadi pada titik waktu tertentu, seperti dalam satu menit, satu jam, atau satu hari ditampilkan pada garis pojok kanan atas
4) Angka 1,312 yang merupakan total analisis DNS

Pemantauan jaringan secara *real-time* memberikan kemudahan bagi *administrator* dalam mengidentifikasi lalu lintas jaringan dan memahami perubahan yang terjadi.

d. Keamanan Jaringan Menggunakan *Sguil*

Pengujian ini dilakukan dengan cara melakukan pengamanan jaringan menggunakan *sguil*.

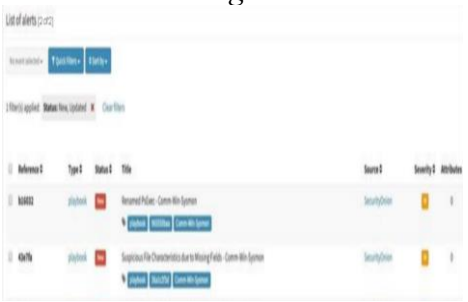


Gambar 44. Tampilan Deteksi *Event*
Sumber: Hasil Tangkapan Layar Penulis (2025)

OSSIM menggunakan *sguil* untuk fungsi keamanan yang berdasarkan hasil pengujian:

1) OSSIM berhasil mendeteksi ancaman secara *real-time*
2) Deteksi serangan berhasil dilakukan oleh *sguil* dengan menampilkan *source* IP, dest IP, dan jenis serangan.

Hasil pemantauan dan keamanan jaringan komputer pada SMAN 11 Luwu menggunakan OSSIM dapat ditampilkan secara detail melalui *sguil*:



Gambar 45. Tampilan Ancaman yang Berhasil diamankan
Sumber: Hasil Tangkapan Layar Penulis (2025)

Dari tampilan gambar peringatan (*alert*) diatas, sistem operasi OSSIM dengan

menggunakan *kibana* dan *sguil* dapat berjalan dengan baik, yang dimana terdapat 2 hasil deteksi ditampilkan pada *kibana* dan dilakukan pengamanan oleh *sguil*, seperti dapat dilihat pada tampilan gambar diatas.

1) OSSIM Melalui *kibana* dan *sguil* berhasil menampilkan hasil deteksi dan pengamanan terhadap ancaman serangan berupa *Rename PsExec* yang merupakan bagian dari teknik serangan aktif, yang artinya dapat memodifikasi file sistem.
2) OSSIM Melalui *kibana* dan *sguil* berhasil menampilkan hasil deteksi dan pengamanan terhadap ancaman serangan berupa *Suspicious file* yang merupakan istilah berbahaya atau mencurigakan yang mirip dengan *malware* yang dapat merusak file sistem.

Ancaman tersebut diamankan bukan dengan diblokir secara langsung atau otomatis, tetapi dengan mendeteksi dan memberikan informasi lengkap kepada *administrator* agar dapat melakukan respon dan tindakan lebih lanjut.

Setelah melalui beberapa pengujian, maka diperoleh hasil dibawah ini:

Tabel 5. Hasil Pengujian system.

No	Indikator Pengujian	Hasil	Ket
1	Kemampuan Sistem Operasi Linux Ubuntu Server 20.04 dalam menjalankan OSSIM	Sistem operasi linux ubuntu server 20.04 baik dalam menjalankan *Open Source Security Information Management* (OSSIM). *Hasil monitoring* ditampilkan melalui *kibana* dan untuk melakukan pemblokiran atau keamanan melalui *sguil*.	Baik
2	Kemampuan OSSIM dalam mengatasi keamanan jaringan komputer SMAN 11 Luwu	Dalam melakukan keamanan jaringan dapat dilakukan berdasarkan alamat *IP Address*. *Sguil* tidak dapat melakukan blokir berdasarkan alamat *url web*.	Baik
3	Kemampuan OSSIM dalam melakukan Monitoring jaringan komputer pada SMAN 11 Luwu	Dalam melakukan *monitoring* lalu lintas data OSSIM dapat melakukannya melalui *dashboard kibana*. Dimana dapat dilakukan monitoring berdasarkan *service* yang digunakan.	Baik

Sumber: Hasil Rancangan Penulis (2025)

Setelah implementasi OSSIM selesai, hasil evaluasi menunjukkan bahwa sistem ini berhasil meningkatkan visibilitas terhadap lalu lintas jaringan secara signifikan dan mempercepat proses deteksi ancaman. OSSIM mampu mengumpulkan *log* dari berbagai perangkat jaringan secara *real-time* dan mengkorelasikan data untuk mendeteksi aktivitas yang mencurigakan.

Hasil nyata yang diperoleh yaitu deteksi serangan dilakukan secara otomatis dan dicatat secara lengkap dalam sistem *log*. *Administrator* menerima *alert* secara *real-time* melalui *dashboard* OSSIM, memungkinkan respon yang lebih cepat terhadap potensi ancaman. Lingkungan jaringan menjadi lebih aman dan terkontrol**,** karena OSSIM memberikan gambaran menyeluruh tentang kondisi keamanan jaringan dan potensi risiko yang ada.

3. Evaluasi (*Evaluating*)

Setelah melakukan tahap tindakan, maka tahap selanjutnya yaitu penulis mengevaluasi hasil pengujian terhadap keamanan sistem *monitoring*. Evaluasi ini dilakukan untuk membandingkan kondisi keamanan jaringan sebelum dan sesudah implementasi, serta menilai kerja OSSIM berdasarkan *log*, laporan, deteksi, dan respon sistem.

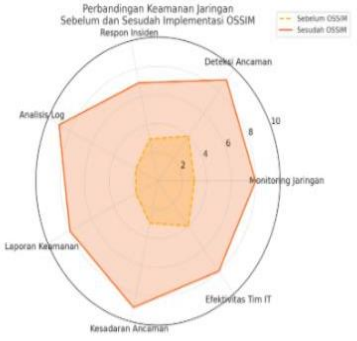
Tabel 6. Perbandingan Kondisi Keamanan Jaringan Sebelum dan Sesudah Implementasi OSSIM

Aspek Keamanan	Sebelum Implementasi OSSIM	Sesudah Implementasi OSSIM
Monitoring Jaringan	Bersifat manual dan terbatas, tidak *real-time*.	Terpusat, *real-time*,
Deteksi Ancaman	Deteksi bersifat reaktif	Deteksi proaktif
Analisis *Log*	*Log* tersebar di berbagai perangkat dan sulit untuk dikorelasikan	Tersedia mekanisme notifikasi otomatis dan skrip respons (otomatisasi dasar).
Laporan Keamanan	Tidak tersedia laporan terintegrasi, sulit untuk dokumentasi dan audit.	Dihasilkan laporan periodik yang informatif, lengkap dengan visualisasi
Kesadaran Ancaman		

EfektivitasTim IT/Security	Rendah, aktivitas tidak terdeteksi atau tidak ditindak. Beban kerja tinggi untuk investigasi manual dan analisis *log* satu per satu.	grafik. Meningkat signifikan, *dashboard* memberi gambaran *real-time* atas kondisi ancaman. Lebih efisien karena sistem membantu dalam pengumpulan data dan deteksi awal.

Sumber: Hasil Rancangan Penulis (2025)

Implementasi OSSIM membawa peningkatan signifikan terhadap sistem keamanan jaringan. Sebelum diimplementasikan, pengawasan dan deteksi ancaman berjalan secara manual, lambat, dan kurang efisien. Setelah OSSIM digunakan, seluruh *log* dapat dikumpulkan secara terpusat, deteksi dilakukan secara otomatis, dan respon terhadap insiden bisa dilakukan lebih cepat dan tepat.



Gambar 46. Skala Perbandingan Keamanan Sebelum dan Sesudah Implementasi OSSIM

Sumber: Hasil Rancangan Penulis (2025)

Gambar tersebut menunjukkan grafik hasil perbandingan antara kondisi keamanan jaringan sebelum dan sesudah implementasi OSSIM. Skala tersebut menggambarkan enam indikator utama yang menjadi tolak ukur dalam menilai tingkat keamanan jaringan, yaitu:

a. Respon insiden: mengukur kemampuan sistem dalam mendeteksi dan merespons insiden keamanana secara cepat dan tepat.
b. Analisis *log*: menunjukkan efektivitas dalam melakukan analisis terhadap catatan aktivitas jaringan.
c. Deteksi ancaman: menggambarkan kemampuan sistem dalam mendeteksi berbagai jenis ancaman.
d. *Monitoring* jaringan: dapat memantau lalu lintas jaringan secara berkelanjutan.
e. Efektivitas tim IT: peningkatan kemampuan tim IT dalam menangani isu keamanan.
f. Kesadaran ancaman: menunjukkan peningkatan pemahaman pengguna jaringan terhadap potensi ancaman.
g. Laporan keamanan: menilai kualitas laporan keamanan yang dihasilkan oleh sistem untuk evaluasi tindak lanjut

Tabel 7. Skala Perbandingan Sebelum dan Sesudah Implementasi OSSIM

Aspek Keamanan	Skala Sebelum Implementasi OSSIM	Skala Sesudah Implementasi OSSIM
Deteksi Ancaman	2,5	8,5
Monitoring	3,0	8,0
Jaringan	2,0	7,5
Analisis *Log*	3,0	8,0
Respon terhadap	2,5	7,5
insiden	2,0	8,0
Kesadaran	3,0	8,5
Ancaman	1,5	8,0
Kecepatan deteksi	1,5	8,0
Visibilitas Jaringan	2,0	7,0
Korelasi data serangan		
Laporan		

Sumber: Hasil Rancangan Penulis (2025)

Berdasarkan tabel diatas, terlihat adanya peningkatan yang signifikan pada seluruh aspek keamanan jaringan setelah implementasi OSSIM di SMAN 11 Luwu. Sebelum OSSIM diimplementasikan, sebagian besar proses deteksi dan monitoring dilakukan secara manual atau bahkan tidak dilakukan sama sekali, yang menyebabkan lambatnya respon terhadap potensi ancaman. Hampir semua aspek keamanan jaringan berada di nilai yang rendah. Namun setelah implementasi selesai, terjadi peningkatan signifikan disemua aspek keamanan.

Setelah OSSIM diimplementasikan, berbagai fitur seperti *log analysis*, *event correlation*, *real-time monitoring*, dan *automatic alerting* terbukti sangat meningkatkan efisiensidan efektivitas sistem keamanan. Skor rata-rata aspek keamanan meningkat dari rentang 2-3 menjadi 7-8,5 setelah implementasi, yang menunjukkan bahwa sistem OSSIM mampu memberikan perubahan nyata dalam perlindungan jaringan disekolah ini.

4. Pembelajaran (Learning)

Tahap terakhir yang dilakukan ini adalah tahap *learning* atau pembelajaran, maka dilakukan *learning* tentang penggunaan hingga pemeliharaan terhadap keamanan sistem *monitoring* kepada pihak SMAN 11 Luwu.

Pembahasan Penelitian

Hasil dari implementasi OSSIM sebagai sistem keamanan jaringan komputer di SMAN 11 Luwu memberikan dampak signifikan terhadap peningkatan kualitas *monitoring* dan deteksi ancaman pada jaringan sekolah. OSSIM mampu melakukan *monitoring* jaringan secara *real-time* menggunakan *tool kibana* yang menampilkan informasi penting seperti alamat IP, jenis layanan yang aktif, serta grafik aktivitas jaringan yang mudah dipahami. Selain itu, sistem juga berhasil mendeteksi berbagai ancaman serangan melalui *tool sguil* dengan bantuan *snort* yang sudah dikonfigurasi dan diaktifkan diawal pada OSSIM. Deteksi dilakukan secara otomatis dan sistem memberikan peringatan (*alert*) secara *real-time* kepada *administrator*, sehingga memungkinkan *respons* yang cepat terhadap ancaman.

Dibandingkan kondisi sebelum implementasi yang bersifat manual dan tidak terintegrasi, OSSIM memberikan kemudahan dan efisiensi yang jauh lebih baik. Evaluasi juga menunjukkan bahwa terdapat peningkatan yang signifikan pada enam aspek utama keamanan jaringan, yaitu *monitoring*, deteksi ancaman, analisis *log*, efektivitas tim IT, kesadaran ancaman, dan pelaporan keamanan. Selain itu, proses transfer pengetahuan kepada pihak sekolah juga berjalan dengan baik, memungkinkan staf SMAN 11 Luwu untuk mengelola dan memelihara sistem OSSIM secara mandiri.

Penelitian sebelumnya menunjukkan bahwa OSSIM memiliki kemampuan yang baik dalam melakukan pemantauan dan deteksi terhadap aktivitas mecurigakan di jaringan komputer. Sistem ini mampu memberikan informasi secara real-time mengenai berbagai ancaman dan kejadian (*event*) yang terjadi dalam jaringan. Namun, kekurangan utama yang ditemukan adalah OSSIM belum mampu melakukan tindakan otomatis dalam mengatasi ancaman yang terdeteksi. Sistem hanya memberikan peringatan dan *log* aktivitas, sehingga respons terhadap serangan tetap memerlukan intervensi manual dari administrator jaringan. Penelitian sebelumnya juga mengungkapkan bahwa OSSIM lebih berperan sebagai alat bantu untuk analisis dan deteksi ancaman daripada sebagai sistem pencegahan aktif. Meskipun demikian, penerapan OSSIM terbukti mampu meningkatkan kesadaran keamanan dan memberikan dampak positif terhadap peningkatan indeks keamanan jaringan, selama didukung oleh keterlibatan aktif administrator dalam mengelola konfigurasi serta merespons ancaman yang muncul.

Namun, ada perbedaan penelitian sebelumnya dengan penelitian ini yaitu penelitian sebelumnya membahas OSSIM dari segi fungsionalitas teknis dan kemampuan deteksi dalam lingkungan laboratorium atau instansi tertentu. Sedangkan, penelitian ini lebih fokus pada implementasi langsung di lingkungan sekolah, yaitu SMAN 11 Luwu. Selain itu, metode yang digunakan dalam penelitian sebelumnya cenderung bersifat konseptual dan teknis, sementara penelitian ini menggunakan metode praktis dengan instalasi, konfigurasi, dan evaluasi langsung

terhadap hasil deteksi ancaman yang muncul. Dengan demikian, penelitian ini memberikan kontribusi nyata dalam bentuk penerapan OSSIM untuk meningkatkan keamanan jaringan di institusi pendidikan.

Secara teknis, implementasi OSSIM memberikan manfaat signifikan dalam pengelolaan keamanan jaringan dengan menyediakan integrasi berbagai fungsi keamanan seperti *Intrusion Detection System* (IDS), *vulnerability assessment*, *event correlation* hingga *monitoring* lalu lintas jaringan dalam satu platform terpadu. Dengan fitur-fitur seperti *log management* dan deteksi serangan *real-time*, OSSIM mampu mengidentifikasi ancaman dengan cepat dan memberikan informasi detail terkait jenis, sumber, dan dampak potensi serangan terhadap sistem. Sementara itu, secara operasional, OSSIM membantu efisiensi dalam pengawasan jaringan dengan menyederhanakan proses analisis data keamanan dalam berbagai sistem, sehingga tim teknis dapat mengambil keputusan yang tepat dan cepat.

Dengan diterapkannya OSSIM, kesadaran keamanan jaringan komputer mendorong adanya upaya pencegahan yang lebih terstruktur dalam menghadapi potensi serangan. Selain itu, melalui hasil monitoring dan analisis log yang tersaji secara visual dan informatif, pihak sekolah lebih cepat merespon kejadian yang mencurigakan. Implementasi ini juga menjadi langkah awal untuk meningkatkan standar keamanan jaringan secara berkelanjutan.

Implementasi OSSIM di SMAN 11 Luwu memiliki beberapa kelebihan, antara lain mampu melakukan *monitoring* jaringan secara *real-time*, mendeteksi ancaman secara otomatis, serta menyajikan data dalam bentuk grafik yang mudah dipahami melalui *kibana* dan *sguil*.

Namun, adapun beberapa kekurangannya yaitu OSSIM tidak secara otomatis memblokir ancaman yang terdeteksi, melainkan hanya memberikan informasi dan peringatan. Tindakan pencegahan terhadap serangan tetap dilakukan manual dari administrator jaringan.

4. KESIMPULAN

Implementasi keamanan jaringan komputer di SMAN 11 Luwu dengan menggunakan OSSIM dilakukan melalui tahapan diagnosing, action planning, action taking, evaluating, dan learning. OSSIM terbukti mampu melakukan monitoring jaringan secara real-time, mendeteksi ancaman secara otomatis, serta memberikan peringatan (alert) kepada administrator. Hasil evaluasi menunjukkan peningkatan signifikan dalam aspek keamanan jaringan. Sistem keamanan jaringan sebelum implementasi OSSIM masih bersifat manual, reaktif, dan terbatas dalam mendeteksi ancaman. Setelah implementasi, proses monitoring menjadi lebih efisien dan terpusat, serta mampu memberikan notifikasi secara otomatis ketika ancaman terdeteksi. Evaluasi perbandingan kondisi sebelum dan sesudah implementasi menunjukkan peningkatan pada semua aspek, mulai dari deteksi ancaman, monitoring jaringan, hingga kesadaran keamanan.

5. DAFTAR PUSTAKA

Apriana, D., & HBH, M. A. (2022). Analisa Jaringan Local Area Network Pada Laboratorium Komputer SMK Informatika Kota Serang. INSANtek, 3(1), 23-31.

Dewantara,R., & Sugiantoro,B. (2021). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus : UIN Sunan Kalijaga Yogyakarta): Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)

Dewanto, R. A., & Suharso, A. (2022). Analisis Teknik-Teknik Kriptografi Terhadap Serangan Jaringan Local. Jurnal Ilmiah Wahana Pendidikan, 8(16), 467-476.

Hanifah, F., Budiyono, A., & Widjajarto, A. (2021). Analisa Kerentanan Pada Vulnerable Docker Menggunakan AlienVault dan Docker Bench For Security

dengan Acuan Framework Cis Control. eProceedings of Engineering, 8(5).

Manalu, A. S., Siregar, I. M., Panjaitan, N. J., & Sugara, H. (2021). Rancang Bangun Infrastruktur Cloud Computing Dengan Openstack Pada Jaringan Lokal Menggunakan Virtualbox. Jurnal Tekinkom (Teknik Informasi dan Komputer), 4(2), 303-311.

Maulana,N.F., & Suartana,I.M. (2024). Simulasi Perancangan Firewall Security Port untuk Implementasi Keamanan Sistem Jaringan di PT. Alfian Jaya Abadi: (Journal of Informatics and Computer Science)

Moningka,G.E., Liando,O.E., & Manggopa,H.K. (2021). Pengaruh penggunaan model pembelajaran berbasis proyek terhadap hasil belajar komputer dan jaringan dasar siswa SMK: Jurnal Pendidikan Teknologi Informasi dan Komunikasi

Pasaribu, M. H. (2021). Implementasi Sebuah Program Berbasis Riset Aksi Dalam Meningkatkan Kualitas program. Education Achievement: Journal of Science and Research, 38-46.

Paw,M.R., Aspriyono,H., & Akbar,A.A. (2024). Implementasi Security Information Dan Event Management (Siem) Dalam Melakukan Monitoring Jaringan Pada SMA 1 Muhammadiyah Boarding School: Jurnal Media Computer Science

Pelealu,R.A., Wonggo,D., & Kembuan,O. (2020). Perancangan dan implementasi jaringan komputer SMK Negeri 1 Tahuna: JOINTER

Putra,A.A., Sapri., & Akbar,A.A. (2022). Penerapan Open Source Security Information Management (OSSIM) Pada Keamanan Jaringan Komputer: jurnal komputer

Simorangkir,S.S., & Harjanti,T.W. (2021). Implementasi Keamanan Jaringan Menggunakan Perangkat Lunak SOPHOS XG Firewall: Jurnal Maklumatika

Susanto, R. (2020). Rancang Bangun Jaringan Vlan dengan Menggunakan Simulasi Cisco Packet Tracer. Jurnal Nasional Informatika Dan Teknologi Jaringan, 4(2), 1-6.

Wijaya, K., Suparianto, R., & Istiawan, E. (2020). Implementasi Framework Bootstrap Dalam Perancangan Sistem Penerimaan Mahasiswa Baru Pada Sekolah Tinggi Ilmu Tarbiyah Al-Quran Al-Ittifaqiah (Stitqi) Indraalayaberbasis Web. JSK (Jurnal Sistem Informasi dan Komputerisasi Akuntansi), 4(2), 7-11.