e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Implementation Of Security Information And Event Management (Siem) In Monitoring Networks At SMA 1 Muhammadiyah Boarding School

Implementasi Security Information Dan Event Management (Siem) Dalam Melakukan Monitoring Jaringan Pada SMA 1 Muhammadiyah Boarding School

M. Reyza Putra Paw [1]; Hari Aspriyono [2]; Abdussalam Al Akbar [3]
[1]Study Program of Informatics, Faculty of Computer Science, Universitas Dehasen Bengkulu
[2,3] Department of Informatics, Faculty of Computer Science, Universitas Dehasen Bengkulu
Email: [1] mreyzaputra@gmail.com

How to Cite :
Paw, M, R, P., Aspriyono, H., Akbar, A, A. (2024). Implementation Of Security Information and Event Management (Siem) In Monitoring Networks At SMA 1 Muhammadiyah Boarding School, Jurnal Media Computer Science, 3(2)

ARTICLE HISTORY
Received [08 Juni 2024]
Revised [09 Juli 2024]
Accepted [11 Juli 2024]

KEYWORDS
SIEM, Monitoring Jaringan, SMA Muhammadiyah Boarding School.

ABSTRAK

Implementasi Security Information Event Managemen (SIEM) Untuk Melakukan Monitoring Jaringan Pada SMA Muhammadiyah Boarding School dapat membantu administrator jaringan mengetahui aktivitas serta status perangkat yang terhubung pada jaringan apakah UP atau Down, dapat membantu memberikan informasi berupa log service yang berjalan dan log security event pada setiap perangkat yang terhubung pada jaringan. Hal ini tentunya dapat mempermudah adminsitrator jaringan dalam menangani permasalahan yang terdapat pada perangkat jaringan yang terhubung ke OSSIM AlienVault. Pada OSSIM AlienVault terdapat platform web UI yang dapat mempermudah administrator jaringan dalam memonitoring jaringan di SMA Muhammadiyah Boarding School. Dimana Web UI OSSIM AlienVault tersebut dapat diakses melalui IP Address Server pada browser. Berdasarkan pengujian yang dilakukan, didapatkan hasil bahwa Implementasi Security Information Event Managemen (SIEM) Untuk Melakukan Monitoring Jaringan Pada SMA Muhammadiyah Boarding School berjalan dengan baik dan dapat membantu administrator jaringan dalam monitoring jaringan serta dapat memberikan informasi berupa log event pada setiap perangkat yang terhubung dalam jaringan.

ABSTRACT

Implementation of Security Information Event Management (SIEM) for Network Monitoring at SMA Muhammadiyah Boarding School can help network administrators know the activity and status of devices connected to the network whether UP or Down, can help provide information in the form of logs of services that run and log security events on each device connected to the network. This of course can make it easier for network administrators to deal with problems found on network devices connected to OSSIM AlienVault. In OSSIM AlienVault there is a web UI platform that can make it easier for network administrators to monitor the network at SMA Muhammadiyah Boarding School. Where the OSSIM AlienVault Web UI can be accessed via the IP Address Server in the browser. Based on the

tests carried out, the results show that the Implementation of Security Information Event Management (SIEM) for Network Monitoring at SMA Muhammadiyah Boarding School runs well and can help network administrators in network monitoring and can provide information in the form of event logs on each device connected to the network.

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 dibidang ini 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 Muhammadiyah Boarding School Kota Bengkulu merupakan salah satu sekolah kejuruan yang ada di Kota Bengkulu dan merupakan salah satu sekolah kejuruan yang menjadi pioneer dalam jurusan Teknik Komputer dan Jaringan. Saat ini SMA Muhammadiyah Boarding School Kota Bengkulu sudah memiliki 2 unit labor komputer yang mana masing-masingnya memiliki 34 unit komputer.

Saat ini Jaringan komputer yang ada pada SMA Muhammadiyah Boarding School Kota Bengkulu 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 serta kerentanan pada jaringan.

Dalam melakukan monitoring banyak *tool* yang dapat digunakan seperti PRTG *Network*, Nagios dan lainnya. Namun pada penelitian ini menggunakan Alientvault yang berbasis linux debian yang dikembangkan oleh AT&T. Dengan adanya penerapan allienvault ini dapat membantu mendefinisikan setiap aset yang terhubung dan memonitoring keamanan pada aset tersebut dalam satu jaringan yang sama, dimana klasifikasi aset seperti host, network, dan services.

LANDASAN TEORI

Analisa

Menurut Kristanto (2019:8) analisa system adalah teknik pemecahan masalah dengan cara memecahkan sistem ke dalam komponen-komponen dengan tujuan mempelajari komponen tersebut bekerja dan berinteraksi untuk menyelesaikan tujuan mereka. Perancangan sistem merupakan pelengkap dari analisa sistem ke dalam suatu sistem yang utuh dengan tujuan mendapatkan sistem yang lebih baik.

Menurut Jefri (2018:82) analisa adalah teknik pemecahan masalah dengan cara memecahkan sistem ke dalarn komponen-komponen dengan tujuan mempelajari komponen tersebut bekerja dan berinteraksi untuk menyelesaikan tujuan mereka. Perancangan sistem merupakan pelengkap dari analisa sistem ke dalam suatu sistem yang utuh dengan tujuan mendapatkan sistem yang lebih baik.

Menurut Yoder (2019: 18) analisa diartikan sebagai prosedur melalui fakta- fakta yang berhubungan dengan setiap pengamatan yang diperoleh dan dicatat secara sistematis.

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Berdasarkan pendapat tersebut maka dalam melakukan suatu analisa perlu dilakukan beberapa prosedur yang berhubungan fakta-fakta yang akan diamati. Adanya prosedur tersebut maka akan terjadinya pemecahan bagian-bagian dalam melakukan suatu pengamatan.

Menurut Muktar (2018:53), Implementasi merupakan sebuah teknik penerapan suatu sistem atau metode guna mendapatkan hasil yang diinginkan dan mengurangi sebuah sistem menjadi bagian – bagian komponen dengan tujuan mempelajari seberapa baik bagian – bagian komponen dengan tujuan yang diharapkan. Analisa sistem merupakan tahapan awal dengan proses pengembangan sistem, sehingga tahapan ini menjadi acuan pelaksanaan pada proses pengembangan sistem.

Menurut Jeffrey (2019:24) Implementasi sistem adalah teknik penerapan suatu metode pada rangkaian sistem dengan tujuan mempelajari komponen tersebut bekerja dan berinteraksi untuk menyelesaikan tujuan dan mendapatkan hasil yang baik.

Perancangan sistem merupakan pelengkap dari analisa sistem ke dalam suatu sistem yang utuh dengan tujuan mendapatkan sistem yang lebih baik. Ada enam tahap analisis sistem:

1. Mengumumkan penelitian sistem. Ketika perusahaan menerapkan sistem baru, manajemen bekerja sama dengan pekerja perihal sistem baru tersebut.
2. Mengorganisasikan tim proyek.
3. Mendefinisikan kebutuhan informasi. Melalui wawancara perorangan, pengamatan, pencarian catatan dan survey.
4. Mendefinisikan kriteria kinerja sistem Setelah kebutuhan informasi manajer didefinisikan, langkah selanjutnya adalah menspesifikasi secara tepat apa yang harus dicapai oleh sistem.
5. Menyiapkan usulan rancangan, Analisa sistem memberikan kesempatan bagi para manajer untuk membuat keputusan terusan atau hentikan untuk kedua kalinya.
6. Menyetujui atau menolak rancangan proyek Manajer dan komite pengarah sistem informasi manajemen mengevaluasi usulan rancangan dan menentukan apakah memberi persetujuan atau tidak.

Jaringan Komputer

Menurut Micro (2019:1) Jaringan komputer adalah sekumpulan peralatan atau komputer yang saling dihubungkan untuk berbagi sumber daya. Agar terjadi jaringan antar komputer maka setiap bagian dari jaringan komputer meminta dan memberikan layanan (servis).Pihak yang meminta layanan disebut client dan yang memberi layanan disebut server.Menurut Pratama (2018:12) Jaringan komputer adalah sekelompok komputer otonom yang dihubungkan satu dengan yang lainnya dengan menggunakan protocol komunikasi melalui media transmisi atau media komunikasi sehingga dapat saling berbagi data inforrnasi, program-program, penggunaan bersama perangkat keras. Seperti printer, hardisk, dan sebagainya.

Dari pendapat ahli diatas dapat disimpulkan Jaringan komputer adalah sekumpulan dua atau lebih komputer yang masing-masing berdiri sendiri dan saling terhubung melalui sebuah teknologi dimana komputer-komputer tersebut dapat bertukar informasi.

Local Area Network (LAN) adalah sejumlah komputer yang saling dihubungkan bersama di dalam satu areal tertentu yang tidak begitu luas, seperti di dalam satu kantor atau gedung. Secara garis besar terdapat dua tipe jaringan atau LAN, yaitu jaringan Peer to Peer dan jaringan Client-Server. LAN tersusun dari beberapa elemen dasar yang meliputi komponen hardware dan software, yaitu:

a. Komponen Fisik
   Personal Computer (PC), *Network Interface Card* (NIC), Kabel, Topologi Jaringan
b. Komponen *Software*
   Sistem Operasi Jaringan, *Network Adapter Driver*, Protokol Jaringan.

LAN merupakan jaringan pribadi di dalam sebuah bangunan sampai beberapa kilometer dari gedung tersebut. LAN banyak digunakan untuk menghubungkan komputer dengan perangkat lain di dalam kantor, perusahaan dan pabrik - pabrik untuk dapat saling berbagi sumber daya dan bertukar informasi. LAN dibedakan dari jenis jaringan lain oleh tiga karakteristik yaitu, teknologi transmisi, ukuran, dan topologi.

Sistem Monitoring

Menurut Pradipta (2020:38) Monitoring jaringan atau *Network Monitoring* adalah penggunaan alat *logging* dan melakukan analisis secara akurat untuk menentukan *trafic flows*, pemanfaatan, dan indikator kinerja lainnya pada sebuah jaringan. Alat pemantauan yang baik memberi nilai pasti dan representasi agregat grafis dari keadaan *real* dari sebuah jaringan. Ini membantu memvisualisasikan dengan tepat apa yang sedang terjadi, sehingga dapat diketahui mana saja penyesuaian yang mungkin diperlukan.

Menurut Fernando (2020:138) Monitoring jaringan merupakan bagian dari manajemen jaringan. Hal yang paling mendasar dalam konsep manajemen jaringan adalah tentang adanya manajer atau perangkat yang memanajemen dan agen atau perangkat yang dimanajemen. Dalam implementasinya, ada berbagai macam arsitektur manajemen jaringan yang didasarkan pada tipe dan ukuran masing-masing. Ada dua arsitektur yang dapat digunakan yaitu manajemen terpusat (*centralized management*) dan manajemen menyebar (*distributed management*). Monitoring jaringan berfungsi sebagai pemantau keadaan jaringan komputer client dan service yang berjalan didalamnya, seperti mengetahui saat komputer dalam keadaan hidup (*up*) dan keadaan mati (*down*).

Monitoring dalam hal ini merupakan proses pengumpulan data dari berbagai sumber yang dilakukan secara real time. Tahapan monitoring secara garis besar dibagi menjadi tiga tahap yaitu:

1. Proses di dalam pengumpulan data monitoring
2. Proses di dalam analisis data monitoring
3. Proses di dalam menampilkan data hasil monitoring

Keamanan Jaringan Komputer

Menurut Munawar (2020:16) Keamanan jaringan komputer melibatkan empat hubungan yang berbeda, yaitu potensi hubungan dengan empat aspek utama ketika menggambarkan bentuk-bentuk ancaman terhadap keamanan jaringan komputer. Ada empat bentuk utama ancaman terhadap keamanan jaringan komputer, penyalahgunaan informasi *Internet of Things*, penolakan layanan serangan latar belakang, kerusakan pada integritas lingkungan jaringan komputer, dan kebocoran informasi komputer.

Menurut Khasanah (2018:183) Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak dimana usaha tersebut bisa dilakukan baik dari dalam maupun dari luar sistem.

Tujuan keamanan komputer meliputi perlindungan informasi dari pihak yang tidak berkepentingan dengan tetap memudahkan akses dan penggunaan oleh para pengguna. Keamanan sistem komputer merupakan mekanisme dan proses kolektif terhadap informasi sensitif dan berharga dan juga layanan yang dilindungi dari publikasi, gangguan atau kehancuran oleh kegiatan yang tidak sah atau individu yang tidak dapat dipercaya dan kejadian-kejadian yang tidak direncanakan masing-masing.

Jenis dan teknik serangan yang mengganggu jaringan komputer beraneka jenis, diantaranya adalah :

1. *Port Scanning*

Merupakan suatu proses untuk mencari dan membuka port pada suatu jaringan komputer. Dari hasil scanning akan didapat letak kelemahan sistem tersebut. Pada dasarnya sistem port

scanning mudah untuk dideteksi, tetapi penyerang akan menggunakan beberapa cara metode untuk menyembunyikan serangan.

2. *Teardrop*

Teknik penyerangan dengan mengeksploitasi proses *disassembly reassembly* paket data. Dalam jaringan internet sering kali data harus dipotong menjadi paket yang lebih kecil untuk menjamin reliabilitas dan proses *multiple* akses jaringan. Pada proses pemotongan data paket yang normal, setiap potongan diberi informasi offset data yang berbunyi "Potongan byte ini merupakan potongan 600 byte dari total 800 byte paket yang dikirimkan". memanipulasi potongan data sehingga terjadi overlapping antara paket yang diterima di bagian penerima setelah potongan-potongan paket disusun kembali.

3. IP *spoofing*

Teknik ini bekerja dengan mengganti alamat IP pengguna yang lain yang bukan penyerang sebenarnya. Hal ini terjadi karena salah rancang (*design flaw*) bagian urutan nomor (*sequence number*) dari paket TCP/IP. Dalam beberapa kasus, penyerang menggunakan satu alamat IP sumber yang spesifik pada semua paket IP yang keluar untuk membuat semua pengembalian paket IP dan pesan ICMP ke pemilik alamat tersebut.

4. ICMP *flood*

Penyerang melakukan eksploitasi dengan tujuan untuk membuat target host menjadi terganggu, yang disebabkan oleh pengiriman sejumlah paket yang besar ke arah target *host*. Eksploitasi sistem ini dilakukan dengan mengirimkan suatu perintah "*ping*" dengan tujuan broadcast atau multicast dimana pengirim dibuat seolah-olah adalah target *host*. Semua balasan dikembalikan ke target *host*.

Hal inilah yang menyebabkan *host* target menjadi terganggu dan menurunkan kinerja jaringan bahkan dapat menyebabkan *Denial Of Service* (DOS).

5. UDP *flood*

UDP *flood* mengaitkan dua sistem tanpa disadari. Dengan cara *spoofing*, *User Datagram Protocol* (UDP) *flood attack* akan menempel pada servis UDP chargen di salah satu mesin, yang untuk keperluan "percobaan" akan mengirimkan sekelompok karakter ke mesin lain, yang diprogram untuk mengecho setiap kiriman karakter yang diterima melalui servis chargen.

Karena paket UDP tersebut di-spoofing diantara ke dua mesin tersebut maka yang terjadi adalah "banjir" tanpa henti paket kiriman karakter yang tidak berguna diantara diantara kedua mesin tersebut. Untuk menanggulangi UDP flood, disable semua servis UDP di semua mesin di jaringan, atau dengan menyaring semua servis UDP yang masuk pada firewall.

Open System Interconnection (OSI) Model

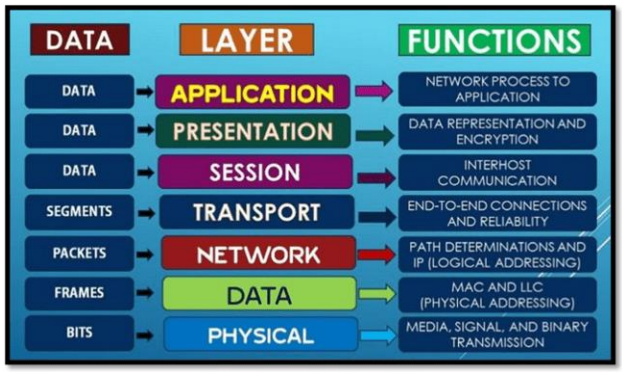
Menurut Iwan (2019:91) Secara umum model OSI membagi berbagai fungsi network menjadi 7 lapisan. Sedangkan lembaga yang mepublikasikan model OSI adalah *International Organization for Standardization* (ISO). Model OSI diperkenalkan pada tahun 1984.

Menurut Pratama (2019:128) *OSI* (*Open System Interconnections*) adalah open sistem yang merupakan himpunan protokol yang memungkinkan terhubungnya dua sistem yang berbeda yang berasal dari arsitektur yang berbeda pula namun dapat juga diartikan senagai suatu group protokol yang membuat dua sistem yang berbeda untuk berkomunikasi tanpa memperdulikan rancangan system dibawahnya. Dibuat oleh *International Standards Organizatio*n (*ISO*). OSI hanya sebuah model protokol, bukan protokol yang bisa dipergunakan.

Dari pendapat ahli diatas dapat disimpulkan *Open Systems Interconnection Reference Model* (Model OSI) merupakan suatu deskripsi abstrak layering untuk rancangan jaringan komputer dan komunikasi, yang dikembangkan sebagai bagian dari *Open Systems Interconnect*.

Biasanya juga disebut sebagai seven OSI layers model. Model OSI membagi fungsi-fungsi dari suatu protokol menjadi beberapa layer. Setiap layer mempunyai properti yang menggunakan fungsi layer dibawahnya, memproses data pada layer tersebut, lalu mengirim ke layer yang selanjutnya. Pada gambar dibawah ini merupakan tujuh layer dari model OSI beserta dengan fungsinya masing-

masing pada setiap layer. Layer pada model OSI dibagi menjadi 2 bagian besar, yaitu layer media dan layer host.



Gambar 1 Tampilan Struktur OSI Model

Protokol Jaringan

Protokol merupakan tata cara atau aturan komunikasi data di dalam jaringan. Untuk melaksanakan komunikasi berbagai macam vendor komputer diperlukan suatu aturan yang standar dan disetujui penerjemah / interpreter atau satu bahasa yang di mengerti kedua belah pihak.

Protokol merupakan sarana komunikasi antara mesin melalui jaringan yang terstandarisasi. Protocol mengizinkan data untuk mengambil bagian dalan transmisi kilat, kemudian ditransmisikan, lalu dikumpulkan kembali sesuai arah dengan perintah yang benar.

Dari uraian ahli diatas dapat disimpulkan Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data Antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya.

Dalam dunia komputer dan telekomunikasi interpreter identik dengan protokol, untuk itu maka badan dunia yang menangani masalah standar ISO (*International Standardization Organization*) membuat demikian yang dimana diharapkan semua vendor perangkat telekomunikasi haruslah berpatokan pada model referensi ini dalampengengembangan protocol tersebut. Pada tingkatan yang terendah, protokol mendefinisikan koneksi perangkat keras. Protocol digunakan untuk menentukan jenis layanan yang akan dilakukan pada internet. Berikut ini tabel yang menjelaskan fungsi setiap layer beserta contoh-contoh protocol yang sesuai untuk masing-masing layer. Adapun protocol-protokol serta fungnyanya berdasarkan layer dapat dilihat pada table 2.1 dibawah ini:

Table 1 OSI Layer

Layer	Fungs	Contoh Protokol
Application	Menyediakan servis bagi aplikasi *Network*	NNTP, HL7, Modbus, SIP, SSI, DHCP, FTP, Gopher, HTTP, HTTPS, NFS, NTP, RTP dan lain sebagainya
Presentation	Mengatur *konversi* dan *translasi* berbagai format data, seperti *kompresi* data dan *enkripsi* data	TDI, ASCII, EBCDIC, MIDI dan lainnya
Session	Mengatur sesi (*Session*) yang meliputi memulai sesi (*Establishing*), mempertahankan sesi (*maintaining*) dan sesi (*terminating*)	SQL, X Window, Named Pipes (DNS), NetBIOS, ASP, SCP dan lainnya
Transport	Menyediakan *end to end*. Layer	TCP, SPX, UDP

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

	bertanggung jawab terhadap keselamatan data dan data.	SCTP dan lainnya
Data Link	Menentukan pengalamatan pendeteksi *error*, kendali aliran *frame* dan *topologi network*	802.3 (Ethernet), 802.11a1b/g/n MAC/LLC, ATM, CDP dan lainnya
Physical	L ini menentuka masalah kelistrikan / gelombang / medan dan berbagai prosedur/fungsi berkaitan dengan *link* pisik	RS-232, V.35, V.34, IOTBASE-T, PORT, SONET dan lainnya

SIEM

Menurut Wardana (2020:46) *Security Information and Event Management* merupakan cara yang digunakan dalam mengatur sebuah jaringan berdasarkan kondisi yang terjadi. Dimana dalam implementasi SIEM banyak tool yang dapat digunakan.

SIEM merupakan sistem yang membantu anda untuk memonitor lalu lintas jaringan dan memberikan analisa secara *real-time* dari *log* yang dihasilkan oleh aplikasi ataupun perangkat keamanan. SIEM merupakan juga sistem manajemen *log* yang mengumpulkan *log* dari berbagai aplikasi dan perangkat keamanan seperti *server*, *network*, *database*, *firewall* dan lain-lain

SIEM mengumpulkan *log* dari aplikasi dan perangkat keamanan yang berbeda dan mengelola itu sebagai sebuah pusat atau biasa disebut *log store*. Biasanya, besaran dari ukuran *log* berdasarkan pada tingkat lalu lintas jaringan. Oleh karena itu, analisis *Big Data* juga memainkan peran penting pada SIEM. Singkatnya, SIEM mengumpulkan semua *log* dari aplikasi / perangkatan keamanan yang berbeda (*log sources*), dan mengolah dan menganalisa log sesuai dengan yang dibutuhkan oleh penggunan SIEM.

Menurut Khotimah (2018:59) *Security Information and Event Management* (SIEM) merupakansistem monitoring yang mampumendeteksi serangan dan respon sistem keamanan terhadap serangan melalui analisis log dari berbagai *event-log* yang bersumber dari data secara *real-time*. *Log* merupakan informasi dari perangkat yang berisi kegiatan dari *log* tersebut, mulai dari lalu lintas jaringan, status dari perangkat dan lainnya.

Ini mungkin proaktif, ketika digunakan untuk mengidentifikasi kerentanan atau berakhirnya sertifikat SSL, atau mungkin reaktif, seperti dalam respons insiden dan forensik jaringan. Baik saat Anda melacak musuh atau berusaha mencegah *malware*, NSM menyediakan konteks, kecerdasan, dan kesadaran situasional dari jaringan Anda. *Enterprise Security Monitoring* (ESM) membawa NSM ke tingkat berikutnya dan mencakup visibilitas titik akhir dan telemetri lainnya dari perusahaan Anda. Ada beberapa solusi komersial yang mendekati apa yang disediakan oleh *Onion Security*, tetapi sangat sedikit yang mengandung kemampuan SIEM dalam satu paket.

Komponen Inti SIEM menyatukan tiga fungsi inti:

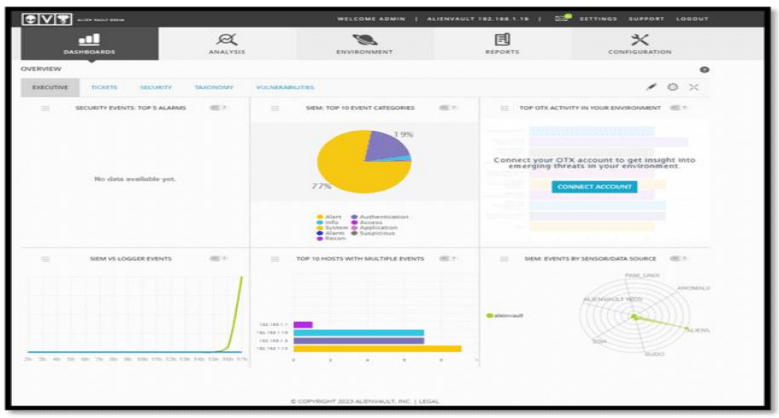
1. Penangkapan paket penuh
2. Sistem deteksi intrusi berbasis jaringan dan berbasis *host* (masing-masing NIDS dan HIDS)
3. Analisis yang kuat.

Tinjauan AlienVault

Menurut Ayuningtyas (2020:2) AlienVault merupakan sistem yang menyederhanakan cara mendeteksi dan merespon ancaman yang terus berkembang saat ini. Pendekatan yang unik dan memenangkan penghargaan organisasi digunakan oleh ribuan pelanggan dan menggabungkan beberapa kontrol keamanan *platform all-in-one*, manajemen keamanan terpadu dengan pertukaran informasi mengenai ancaman yang terbuka. Ancaman bersumber dari komunitas intelijen untuk mendeteksi ancaman dan mencari cara yang efektif dan berkesinambungan dan agar dapat dicapai

oleh tim IT yang terbatas dengan sumber daya. Fitur-fitur AlienVault yaitu *Asset Discovery*, *Vulnerability Assessment*, *Behavioral Monitoring*, *Intrusion Detection*, dan *SIEM*.

SIEM juga merupakan sistem keamanan yang komprehensif yang mencakup open source dari deteksi untuk menghasilkan metrik dan laporan ke tingkat eksekutif. AlienVault ditawarkan sebagai produk keamanan yang memungkinkan untuk mengintegrasikan ke dalam satu konsol, semua perangkat keamanan dan alat yang dimiliki di jaringan, dan pemasangan alat-alat *open source* seperti *Snort*, *openvas*, *ntop* dan *OSSEC*. Cara kerjanya adalah sistem melakukan penilaian risiko untuk setiap peristiwa dan hubungan yang terjadi. Selama proses korelasi, dari serangkaian pola, menghasilkan mekanisme baru untuk mendeteksi serangan atau masalah dengan jaringan.



Gambar 2 Tampilan Tool AlienVault

Komputer

Sedangkan menurut Zahir (2019:2) Komputer merupakan serangkaian ataupun sekolompok mesin elektronik yang terdiri dari ribuan bahkan jutaan komponen yang dapat saling bekerja sarna, serta membentuk sebuah system kerja yang rapi dan teliti. Sistem ini kemudian dapat digunakan untuk melaksanakan serangkaian pekerjaan secara otomatis, berdasarkan urutan instruksi ataupun program yang diberikan kepadanya.

Komputer adalah alat yang dipakai untuk mengolah informasi menurut prosedur yang telah dirumuskan. Tujuan penggunaan komputer adalah agar setiap data yang diolah dapat dihasilkan informasi yang cepat, akurat, dan efisien.

Komputer juga dapat diartikan sebagai alat yang dipakai untuk mengolah data menggunakan sebuah program. Program sendiri adalah prosedur yang telah dirumuskan.

Fungsi utama komputer meliputi pengolahan data, penyimpanan data, pemindahan data dan kontrol. Komputer memiliki empat struktur utama, yaitu:

a. CPU (*central processing unit*), berfungsi mengontrol operasi di dalam komputer dan membentuk fungsi-fungsi pengolahan data.
b. Memory, berfungsi untuk menyimpan data.
c. I/O (*input output*), berfungsi memindahkan data.
d. *Interconnection System*, berfungsi untuk mengatur mekanisme komunikasi antara CPU, memory dan I/O.

Secara prinsip, komputer hanyalah merupakan sebuah alat yang bias digunakan untuk membantu manusia dalam menyelesaikan pekerjaanya. Untuk bisa bekerja, alat tersebut memerlukan adanya program dan manusia. Pengertian manusia kemudian dikenal dengan istilah *brainware* (perangkat manusia).

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

METODE PENELITIAN

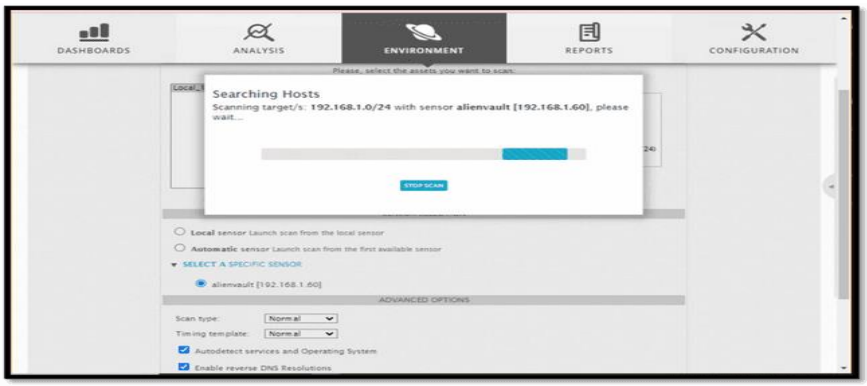
Metode penelitian yang digunakan, yaitu penelitian eksperimen. Penelitian dengan pendekatan eksperimen adalah suatu penelitian yang berusaha mencari pengaruh variabel yang lain dalam kondisi yang terkontrol. Metode penelitian yang dilakukan dalam penelitian ini yaitu dengan menggunakan metode eksperimen langsung untuk membangun sebuah sistem monitoring dan keamanan jaringan komputer dengan menggunakan SIEM pada SMA 1 Muhammadiyah Boarding School Kota Bengkulu.

HASIL DAN PEMBAHASAN

Implementasi *Security Information Event Managemen* (SIEM) Untuk Melakukan *Monitoring* Jaringan Pada SMA Muhammadiyah Boarding School dilakukan selama 2 minggu mulai dari Tanggal 12 Februari 2024 sampai dengan 26 Februari 2024. OSSIM AlienVault di hubungkan pada jaringan komputer di SMA Muhammadiyah Boarding School, seperti terlihat pada Gambar 3.

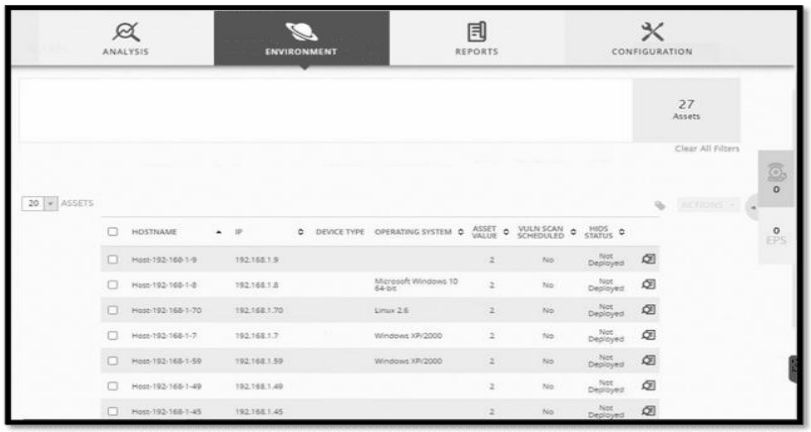
Gambar 3 Implementasi OSSIEM AlienVault Di SMA Muhammadiyah Boarding School

Kemudian melakukan scanning untuk mendeteksi semua aset yang terhubung dalam jaringan yang terdapat di SMK Muhammadiyah Boarding School, seperti terlihat pada Gambar 4.



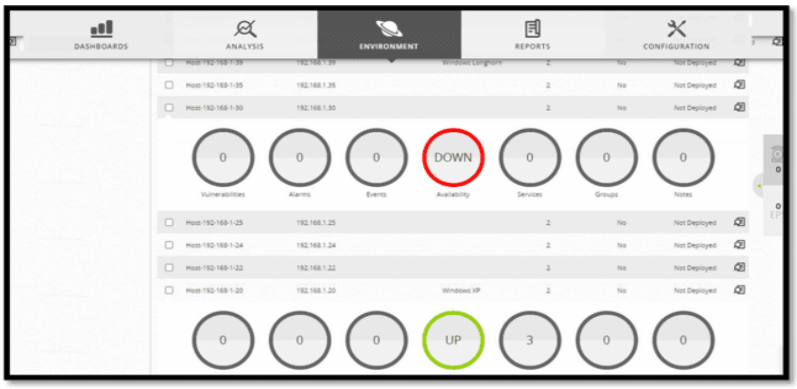
Gambar 4 Scaning Asset Jaringan Di SMA Muhammadiyah Boarding School

Dari hasil scaning yang telah dilakukan terdapat 27 aset yang terdefinisi oleh OSSIEM AlienVault seperti terlihat pada Gambar 4.



Gambar 5 Hasil Scaning Aset Jaringan Di SMA Muhammadiyah Boarding School

Setelah itu melakukan monitoring pada setiap asset yang telah di scanning oleh AllienVault, dimana terlihat ada beberapa device yang Up dan ada device yang down, seperti terlihat pada Gambar 6.



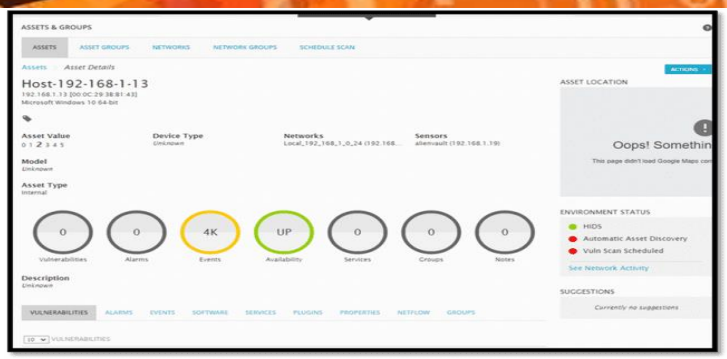
Gambar 6 Monitoring Asset Jaringan di SMA Muhammadiyah Boarding School

Kemudian mengaktifkan vulnerability scan dengan mengatur metode scaning untuk mendeteksi keamanan pada asset yang di monitoring dengan cara seperti terlihat pada Gambar 7.

Gambar 7 Vulnerability Scan Pada Aset

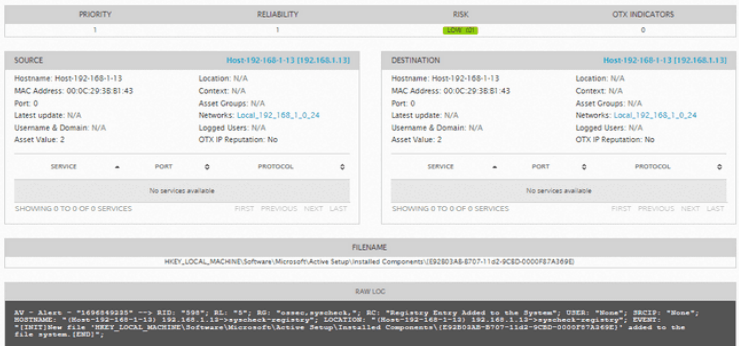
Aset yang telah terhubung dan dimonitoring oleh AlienVault seperti terlihat pada Gambar 8.

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE



Gambar 8 Aset Host-192.168.1.13

Monitoring dapat dilakukan dengan melihat log event yang telah dimonitoring oleh AlienVault pada host-192.168.1.13 tersebut. Pada setiap log event, administrator jaringan dapat melihat informasi lebih detail terkait dengan event yang dimonitoring, seperti terlihat pada Gambar 4.7.



Gambar 9 Detail Log Event

Selain itu OSSIM AlienVault dapat mengetahui kondisi status Up/Down pada setiap host device yang terhubung pada jaringan, seperti terlihat pada Gambar 10.

Gambar 10 Kondisi Status Availability Pada Host Device

Pada OSSIM AlienVault terdapat 3 level kategori risk vurnerability, antara lain :

1. Low Risk (berwarna hijau) merupakan kategori risk termasuk aman atau tidak adanya kerentanan yang terjadi di dalam jaringan dan memiliki skor yang bernilai 1.
2. Medium Risk (berwarna kuning) merupakan kateogir risk yang termasuk peringatan dalam pantauan yang mengharuskan pihak administrator jaringan untuk melihat informasi kerentanan yang diberikan di dalam jaringan dam memiliki skor yang bernilai 2.

3. High Risk (berwarna merah) merupakan kategori risk yang termasuk berbahaya yang mengharuskan pihak administrator segera mengatasi kerentanan yang terjadi berdasarkan hasil monitoring yang dilakukan di dalam jaringan dan memiliki skor yang bernilai lebih dari 3

Setelah melakukan monitoring OSSIM AllienVault pada Jaringan di SMA Muhammadiyah Boarding School, terdapat beberapa kendala yang dirasakan antara lain :

1) Asset yang telah berhasil di Scan oleh AllienVault yang berada pada range 192.168.1.0/24 melalui sensor server AllienVault, tidak diketahui komputer/laptop mana saja yang terdeteksi sehingga perlu dilakukan pengecekan ulang pada setiap komputer/laptop yang terhubung pada jaringan di SMK Muhammadiyah Boarding School satu persatu untuk mengetahui IP Address yang didapatkan dan kemudian disamakan dengan IP Address hasil scaning OSSIM AllienVault, sehingga membutuhkan waktu yang cukup lama.
2) Selama melakukan monitoring jaringan pada SMA Muhammadiyah Boarding School, hasil deteksi keamanan menunjukkan tidak adanya ancaman yang tinggi atau *low risk* yang terjadi pada setiap Asset yang terdeteksi oleh OSSIM AlienVault.

Tabel 2 Hasil Pengujian

No	Indikator	Hasil	Ket
1	Kemampuan SIEM dalam melakukan monitoring Aktifitas pada jaringan UP/Down perangkat yang terhubung pada jaringan	OSSIM AlienVault mampu melakukan monitoring dan memberikan informasi kondisi setiap perangkat yang terhubung	Berhasil
2	Kemampuan SIEM dalam menampilkan log service, log event pada setiap perangkat yang terhubung pada jaringan	Pengujian NMap berhasil dilakukan dan terdeteksi pada SIEM AlienVault pada log event, namun serangan tersebut masih berisiko low risk	Berhasil
		Pengujian LopthCrack berhasil dilakukan namun tidak terdeteksi pada SIEM AlienVault.	Tidak Berhasil
		Pengujian LOIC hanya dapat melakukan permintaan (requested) tanpa adanya feedback, sehingga tidak berhasil dan tidak terdeteksi SIEM AlienVault	Tidak Berhasil

Berdasarkan pengujian yang dilakukan, didapatkan hasil bahwa Implementasi Security Information Event Managemen (SIEM) Untuk Melakukan Monitoring Jaringan Pada SMA Muhammadiyah Boarding School, antara lain :

1) Selama melakukan monitoring jaringan pada SMA Muhammadiyah Boarding School, hasil deteksi keamanan menunjukkan tidak adanya ancaman yang tinggi atau *low risk* yang terjadi pada setiap Asset yang terdeteksi oleh OSSIM AlienVault.
2) Dapat membantu administrator jaringan dalam monitoring jaringan serta dapat memberikan informasi berupa log event pada setiap perangkat yang terhubung dalam jaringan.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil dan pembahasan serta pengujian, maka dapat disimpulkan bahwa :

1. Implementasi Security Information Event Management (SIEM) Untuk Melakukan Monitoring Jaringan Pada SMA Muhammadiyah Boarding School dapat membantu administrator jaringan mengetahui aktivitas serta status perangkat yang terhubung pada jaringan apakah Up atau Down, dapat membantu memberikan informasi berupa log service yang berjalan dan log security event pada setiap perangkat yang terhubung pada jaringan. Hal ini tentunya dapat mempermudah adminsitrator jaringan dalam menangani permasalahan yang terdapat pada perangkat jaringan yang terhubung ke OSSIM AlienVault.
2. Pada OSSIM AlienVault terdapat platform web UI yang dapat mempermudah administrator jaringan dalam memonitoring jaringan di SMA Muhammadiyah Boarding School. Dimana Web UI OSSIM AlienVault tersebut dapat diakses melalui IP Address Server pada browser.
3. Berdasarkan pengujian yang dilakukan, didapatkan hasil :

a. Asset yang telah berhasil di Scan tidak dapat diketahui komputer/laptop mana saja yang terdeteksi sehingga perlu dilakukan pengecekan ulang pada setiap komputer/laptop yang terhubung jaringan di SMA Muhammadiyah Boarding School satu persatu untuk mengetahui IP Address dan kemudian disamakan dengan IP Address hasil scaning OSSIEM AllienVault, sehingga membutuhkan waktu yang cukup lama.
b. Selama melakukan monitoring jaringan pada SMA Muhammadiyah Boarding School, hasil deteksi keamanan menunjukkan tidak adanya ancaman yang tinggi atau *low risk* yang terjadi pada setiap Asset yang terdeteksi oleh OSSIEM AlienVault.
c. Dapat membantu administrator jaringan dalam monitoring jaringan serta dapat memberikan informasi berupa log event pada setiap perangkat yang terhubung dalam jaringan

Saran

Berdasarkan kesimpulan, maka penulis menyarankan untuk penelitian selanjutnya dilakukan pengembangan terhadap OSSIEM AlienVault dengan menambahkan beberapa sensor range agar dapat mendeteksi seluruh aset dalam jaringan, dan juga perlu adanya definisi terkait IP Address komputer/laptop pada setiap aset agar diketahui owner aset mana saja yang terdeteksi oleh AlienVault sehingga mempermudah administrator jaringan melakukan pengecekan dan memberikan informasi.

DAFTAR PUSTAKA

Ahmad. S Abdullah. 2019. *Analisis Quality Of Service (QoS) pada Wireless Local Area Network (WLAN) AD – Hoc dengan menggunakan antena buatan*. Program Studi Sistem Informasi Universitas Gajah Mada. Yogyakarta

Alfatah, Dedi Muhammad. 2019. *Pengaruh Kualitas Jaringan Internet Terhadap Kepuasan Pelanggan Indihome PT. Telkom*. Jurnal Imiah Pendidikan dan Pembelajaran. p-ISSN : 1858-4543 e-ISSN : 2615-6091. Program Studi Magister Teknologi & Kejuruan, Fakultas Teknik, Universitas Negeri Padang

Dasanty, Laras Vriella. 2020. *Studi Literatur Monitoring Manajemen Jaringan Internet Dengan Konsep SNMP Terhadap Akses Siswa*. Jurnal IT-EDU. Pendidikan Teknologi Informasi, Fakultas Teknik, Universitas Negeri Surabaya

Fahlepi, Roma Doni. 2018. *Jaringan Komputer Dari Jarak Jauh Dengan Penerapan Hamachi VPN*. Jurnal Evolusi. Universitas Bina Sarana Informatika

Februrian. 2020. *Membangun Dan Menguji Web Browser Dan Server Pada Onion Web Server (Deepweb)*. Jurnal JARKOM. E-ISSN: 2338-6304. Institut Sains & Teknologi AKPRIND. Yogyakarta

Ferdiansyah, Pramudhita. 2020. *Analisis Manajemen Bandwidth Menggunakan Hierarchical Token Bucket Pada Router dengan Standar Deviasi*. Jurnal Nasional Teknologi dan Sistem Informasi. ISSN 2460-3465. Universitas Amikom Yogyakarta.

Hariyadi, I Putu. 2018. *Analisa Penerapan Private Cloud Computing Berbasis Proxmox Virtual Environment Sebagai Media Pembelajaran Praktikum Manajemen Jaringan*. Jurnal MATRIK. p-ISSN. 1858-4144. STMIK Bumigora. Nusa Tenggara Barat

Jeffrey, A Denzi. 2017. *Handbook of Qualitative Research*. Pustaka Pelajar. Yogyakarta

Muktar, Ahmad. 2018. *Authentic Assessment: Penilaian Berbasis Kelas dan Kompetensi*. Refika Aditama. Bandung

Muzakir, Muhammad. 2019. *Optimasi Kinerja Jaringan Menggunakan HSRP (Hot Standbye Router Protocol)*. Bina Darma Conference on Computer Science. Fakultas Teknik Ilmu Komputer, Universitas Bina Darma

Pradikta, Jurista Purnama. 2018. *Perancangan Sistem Monitoring Konsultasi Bimbingan Akademik Mahasiswa dengan Notifikasi Realtime Berbasis SMS Gateway*. Jurnal Media Informatika Budidarma. ISSN 2614-5278. Fakultas Teknologi Komunikasi dan Informasi, Informatika, Universitas Nasional. Jakarta

Pratama, I Putu Agung. 2016. *Handbook Jaringan Komputer – Edisi Revisi*. Graha Ilmu. Yogyakarta

Purbo, Onno W. 2019. *Macam-macam Tool Yang Dapat Digunakan Dalam Melakukan Monitor Jaringan Berbasis Open Source*. Mediacom. Bandung

Santoso, Akhmad. 2019. *Koneksi Internet Dengan Modem Handphonepada Sistem Operasi Linux Ubuntu (Studi Kasus Pada SMA N 2* Semarang*)*. Jurnal Ilmiah Fakultas Ilmu Terapan, Universitas Sains dan Teknologi(STEKOM). Semarang