Perancangan Dan Implementasi Sistem Keamanan Jaringan Menggunakan Alienvault Pada SMK N 4 Kota Bengkulu

[1]Gita Dahlia Lestari, [2]Juju Jumadi, [3]Ahmad Asyhari

[1] Mahasiswa, Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu
Alamat: Desa cahaya batin kecamatan semidang gumay kabupaten kaur
e-mail: dahliagita46@gmail.com
[2,3] Dosen Tetap, Program Studi Informatika Ilmu Komputer, Universitas Dehasen Bengkulu
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139;
e-mail: juju.jumadi@unived.ac.id , ahmadasyhari@unived.ac.id

(Received: Nopember 2025, Revised: Februari 2026, Accepied: April 2026)

Abstract-This study aims to design and implement a network security system using AlienVault OSSIM at SMK N 4 Kota Bengkulu. The method used in this research is the Network Development Life Cycle (NDLC), which consists of analysis, design, simulation, implementation, monitoring, and management stages. AlienVault is implemented as a standalone operating system running on a virtual machine using VMware and is utilized to perform centralized network monitoring, threat detection, and security management. System testing is conducted using the black box method by simulating attacks such as port scanning and ping flooding. The test results show that AlienVault is capable of detecting network activities, identifying connected devices, and providing alerts for suspicious activities. With the implementation of this system, network security at SMK N 4 Kota Bengkulu becomes more controlled, secure, and supportive of teaching and learning activities.
Keywords: Network Security, AlienVault OSSIM, NDLC, Network Monitoring, Intrusion Detection System

Abstrak-Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan jaringan menggunakan AlienVault OSSIM pada SMK N 4 Kota Bengkulu. Metode yang digunakan dalam penelitian ini adalah Network Development Life Cycle (NDLC) yang meliputi tahapan analisis, perancangan, simulasi, implementasi, monitoring, dan manajemen. AlienVault diimplementasikan sebagai sistem operasi tersendiri yang dijalankan pada mesin virtual menggunakan VMware dan digunakan untuk melakukan monitoring, pendeteksian ancaman, serta pengamanan jaringan secara terpusat. Pengujian sistem dilakukan menggunakan metode black box dengan melakukan simulasi serangan seperti port scanning dan ping flooding. Hasil pengujian menunjukkan bahwa AlienVault mampu mendeteksi aktivitas jaringan, mengidentifikasi perangkat yang terhubung, serta memberikan peringatan terhadap aktivitas mencurigakan. Dengan diterapkannya sistem ini, keamanan jaringan di SMK N 4 Kota Bengkulu menjadi lebih terkontrol, aman, dan mendukung kegiatan belajar mengajar secara optimal.
Kata kunci: Keamanan Jaringan, AlienVault, NDLC, Monitoring Jaringan, SMK N 4 Kota Bengkulu.

1. PENDAHULULUAN

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, disiplin ilmu di bidang ini juga semakin beragam sesuai dengan kebutuhan perkembangan ilmu itu sendiri. Demikian pula, ancaman terhadap keamanan sistem jaringan berkembang seiring dengan meningkatnya pemanfaatan teknologi tersebut. Sistem jaringan sering menghadapi berbagai kekurangan, di antaranya gangguan berupa virus, komputer yang bermasalah, atau serangan dari luar yang dapat berupa berbagai bentuk *attacking network system*. Gangguan dari dalam jaringan pun bisa terjadi, misalnya karena adanya otoritas yang melakukan perbaikan sistem atau pengolahan data sehingga meninggalkan gangguan seperti virus atau koneksi yang *down*. SMK N 4 Kota Bengkulu merupakan salah satu sekolah kejuruan yang ada di Bengkulu dan menjadi pelopor dalam jurusan Teknik Komputer dan Jaringan. Saat ini SMK N 4 Kota Bengkulu telah memiliki 2 laboratorium, yang mana laboratorium 1 memiliki 25 unit komputer dan laboratorium 2 memiliki 23 komputer. Jaringan komputer di sekolah ini sudah berjalan sesuai kebutuhan untuk menunjang kegiatan belajar dan mengajar. Namun, pengamanan jaringan saat ini masih bersifat personal pada masing-masing komputer dan belum memiliki sistem monitoring serta keamanan yang bersifat keseluruhan. Akibatnya, sering terjadi berbagai masalah, seperti jaringan *down*, performa jaringan menurun, virus menyebar, siswa/i bebas mengakses situs yang tidak sesuai, serta perlunya perlindungan terhadap data penting di ruangan Tata Usaha. Kondisi ini membuat jaringan rentan terhadap gangguan baik dari dalam maupun luar sistem. Beberapa permasalahan yang muncul antara lain kurangnya monitoring jaringan secara menyeluruh, keamanan yang masih bersifat personal pada masing-masing komputer, akses internet siswa yang belum dibatasi, serta perlunya proteksi terhadap data penting di ruangan Tata Usaha. Kondisi ini menunjukkan perlunya implementasi sistem keamanan jaringan yang terintegrasi. Dalam melakukan keamanan jaringan, banyak tool yang dapat digunakan, seperti *PRTG Network*, *Nagios*, dan lainnya. Untuk keamanan jaringan, terdapat juga sistem seperti *IDS (Intrusion Detection System)* yang mampu mendeteksi serangan *DOS, CGI attack*, *SQL injection*, dan lain-lain. Namun, untuk dapat melakukan monitoring sekaligus keamanan jaringan secara bersamaan, salah satu solusi yang dapat digunakan adalah *AlienVault*. *AlienVault* merupakan software sumber terbuka yang gratis dan mampu melakukan monitoring serta pengamanan jaringan secara terpadu. Berdasarkan latar belakang di atas, penulis tertarik mengambil judul "Perancangan dan Implementasi Sistem Keamanan Jaringan Menggunakan Alienvault pada SMK N 4 Kota Bengkulu", dengan tujuan merancang dan

mengimplementasikan sistem keamanan jaringan yang dapat berjalan secara terintegrasi, sehingga jaringan komputer di SMK N 4 Kota Bengkulu menjadi lebih aman, stabil, dan terlindungi dari berbagai ancaman.

II. TINJAUAN PUSTAKA

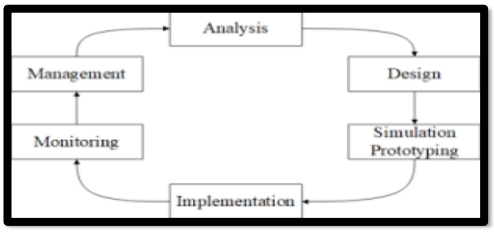
Menurut Wilujeng (2024:2681) Jaringan komputer adalah sekumpulan peralatan atau komputer yang saling dihubungkan untuk berbagi sumber daya. Agar terjadi jaringan antar komputer maka setiap bagian dari jaringan komputer meminta dan memberikan layanan (*servis*). Pihak yang meminta layanan disebut client dan yang memberi layanan disebut *server*. Menurut Prtnomo (2024:2045) 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 Khairunnisa (2024:10) 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. Menurut Abdullah (2020:6880) 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.

III. METODOLOGI PENELITIAN

Dalam Penelitian skripsi ini penulis menggunakan metode *Network Development Life Cycle* (NDLC). Metode *Network Development Life Cycle* (NDLC) merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup pengembangan aplikasi, dan analisis pendistribusian data.

Adapun tahapan NDLC dapat dilihat pada gambar dibawah ini ;



Gambar.1 Tahapan *Network Development Life Cycle* (NDLC)

Table.1 Rencana Pengujian

No	Indikator Pengujian	Hasil yang Diharapka	KET
1	Kemampuan AlienVault dalam mendeteksi aktivitas port scanning	Sistem mampu mendeteksi dan menampilkan peringatan (alert) serangan port scanning	Berhasil / Tidak
2	Kemampuan AlienVault dalam memantau lalu lintas jaringan (Traffic Monitoring)	Aktivitas jaringan dapat dipantau secara real-time	Berhasil / Tidak
3	Respons AlienVault terhadap serangan ping flooding (ICMP flood)	Sistem mampu memberikan peringatan dan mencatat log serangan	Berhasil / Tidak
4	Kemampuan AlienVault dalam mendeteksi serangan brute force pada layanan SSH	Sistem mampu mendeteksi percobaan login berulang dan menampilkan alert	Berhasil / Tidak
5	Stabilitas AlienVault yang dijalankan pada mesin virtual (VMware/VirtualBox)	Sistem berjalan stabil tanpa gangguan selama proses pengujian	Berhasil / Tidak

P-ISSN 1858-2680
E-ISSN 2723-4673

IV. HASIL DAN PEMBAHASAN

A.Hasil

Tahap hasil penelitian ini menjelaskan proses penerapan, pengujian, serta hasil observasi dari implementasi sistem keamanan jaringan menggunakan AlienVault OSSIM 4.13.0 yang diintegrasikan dengan Suricata IDS. Penelitian ini dilaksanakan pada SMK Negeri 4 Bengkulu, dengan tujuan utama membangun sistem monitoring dan keamanan jaringan terpusat yang dapat mendeteksi aktivitas normal maupun serangan siber secara real-time.

Sebelum penerapan sistem keamanan berbasis OSSIM, jaringan di SMK Negeri 4 Bengkulu menghadapi berbagai permasalahan, antara lain: Tidak adanya istem monitoring terpusat. Setiap perangkat bekerja secara independen, sehingga administrator kesulitan mengetahui status jaringan secara keseluruhan. Sering terjadi gangguan jaringan (down) tanpa terdeteksi sumbernya. Hal ini disebabkan tidak adanya sistem logging dan analisis lalu lintas yang komprehensif. Keamanan data belum terjamin. Akses internet oleh siswa masih bebas tanpa pembatasan situs, menyebabkan potensi malware dan serangan siber meningkat. Data aset jaringan belum terdokumentasi dengan baik. Banyak perangkat aktif di jaringan tanpa tercatat di sistem manajemen aset, menyebabkan kesulitan saat proses deteksi dan monitoring.

Permasalahan di atas menjadi dasar pentingnya penerapan AlienVault OSSIM sebagai Security Information and Event Management (SIEM) yang dapat mengintegrasikan semua log dan peringatan keamanan dalam satu platform.

Hasil penelitian disusun berdasarkan pendekatan Network Development Life Cycle (NDLC) yang terdiri dari enam tahap: analysis, design, simulation prototyping, implementation, monitoring, dan management. Setiap tahap menghasilkan keluaran yang menjadi dasar dari pengujian dan pembahasan sistem secara keseluruhan.

Instalasi AlienVault di Vmware

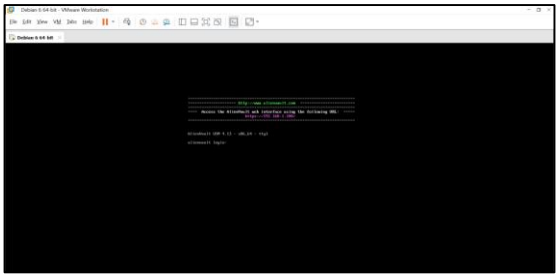
Proses instalasi dilakukan dengan menambahkan file ISO AlienVault OSSIM ke dalam VMware Workstation. Sistem operasi dasar yang digunakan adalah Debian 6 (64-bit) sesuai dengan requirement AlienVault versi 4.1.3.0. Setelah instalasi selesai, AlienVault dijalankan dengan dua interface jaringan: eth0 sebagai interface manajemen (IP 192.168.1.100) dan eth1 sebagai interface monitoring. Konfigurasi ini bertujuan agar satu interface khusus digunakan untuk komunikasi administrasi, sedangkan interface lain difokuskan untuk melakukan sniffing traffic dan deteksi serangan.

Gambar 4.1 Instalasi AlienVault

Gambar . Instalasi AlienVault

Dalam implementasinya, digunakan dua buah interface jaringan (NIC):

1. eth0 → interface manajemen (IP 192.168.1.100) digunakan untuk login web GUI dan administrasi.
2. eth1 → interface monitoring, berfungsi untuk melakukan sniffing traffic jaringan dan mendeteksi serangan.



Gambar 3. Mengkonfigurasi Jaringan

Konfigurasi dual-interface ini memastikan pemisahan fungsi antara manajemen dan monitoring sehingga sistem lebih aman dan efisien.

Setelah proses instalasi selesai, sistem dijalankan dan dilakukan konfigurasi awal untuk menetapkan:

1. IP Address eth0: 192.168.1.100 (akses manajemen)
2. Hostname: alienvault.local
3. Service aktif: ossim-agent, ossim-server, suricata

 P-ISSN 1858-2680
E-ISSN 2723-4673

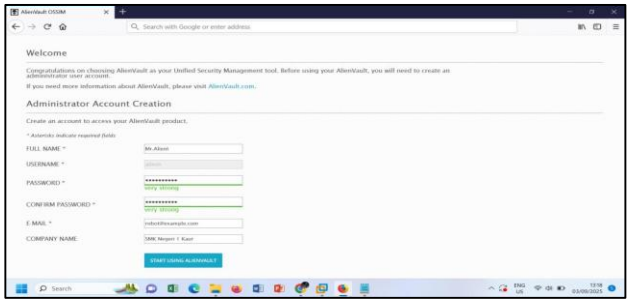
Sistem kemudian diuji untuk memastikan semua service aktif menggunakan perintah:

1. sudo /etc/init.d/ossim-agent status
2. sudo /etc/init.d/ossim-server status
3. sudo /etc/init.d/suricata status

Semua service terdeteksi aktif dan siap digunakan.

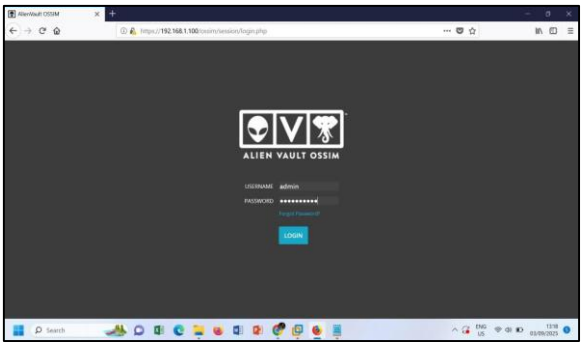
Login ke AlienVault Web GUI

Setelah instalasi berhasil, pengguna dapat mengakses web GUI AlienVault melalui browser dengan alamat https://192.168.1.100. Proses login menggunakan akun administrator yang telah dibuat sebelumnya. Web GUI ini menjadi pusat monitoring, konfigurasi sensor, serta tempat analisis log dan event. Dari antarmuka ini administrator dapat melihat status sensor, daftar aset, hingga laporan keamanan secara real-time.

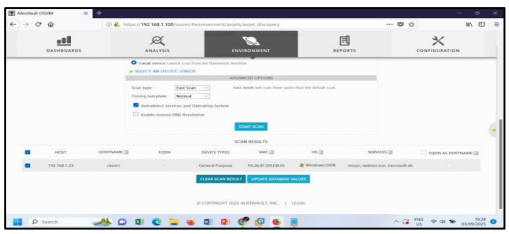


Gambar 4 Login AlienVault Via Console Sekaligus Server

Login dilakukan menggunakan akun administrator yang sudah dibuat pada tahap instalasi. Web GUI ini berfungsi sebagai:



Gambar 5. Administrator Account Creation



Gambar 6. Login AlienVault via WebGuy

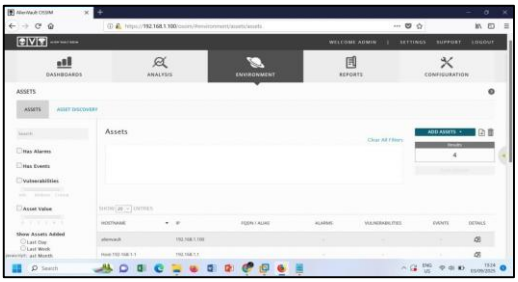
Setelah login menggunakan akun administrator, halaman utama menampilkan berbagai menu seperti: Dashboard: Tampilan ringkasan keamanan jaringan. Analysis: Menampilkan event keamanan dan log deteksi Suricata. Assets: Menampilkan daftar perangkat (host) yang terdeteksi dalam jaringan. Configuration: Pengaturan sensor, plugin, dan koneksi antar komponen OSSIM.

Penambahan Aset

Langkah pertama dalam pengujian adalah menambahkan aset jaringan (client atau server) ke dalam AlienVault. Penambahan aset dilakukan melalui menu Assets pada dashboard. Setiap aset yang didaftarkan akan memiliki profil tersendiri sehingga setiap aktivitas yang berasal dari aset tersebut dapat dimonitor secara spesifik.

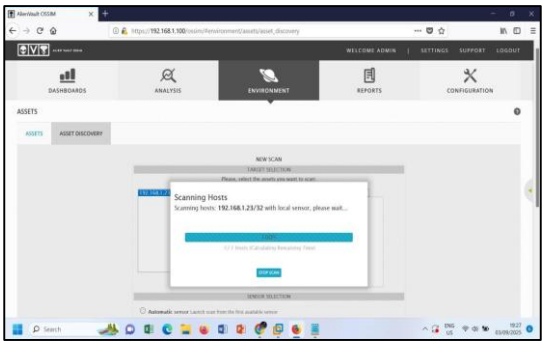
Aset yang ditambahkan meliputi:

1. Client Windows,
2. Kali Linux (attacker machine),
3. AlienVault OSSIM (server IDS/IPS).



Gambar 7. Penambahan Aset Client

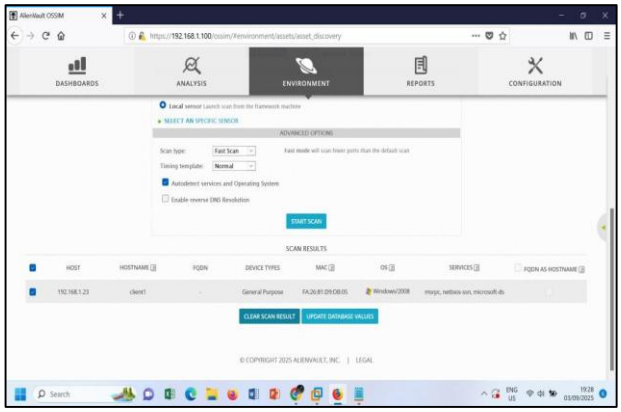
Penambahan aset dilakukan melalui menu Assets → New Asset pada dashboard. Setiap aset memiliki profil spesifik yang akan dicatat sehingga aktivitas jaringan antar-aset dapat dimonitor secara detail.



Gambar 8. Scanning Hosts Clinet Yang Ditambahkan

Dari hasil konfigurasi, seluruh perangkat yang terhubung pada jaringan LAN — termasuk server AlienVault, client Windows, dan Kali Linux (attacker) — berhasil ditambahkan melalui menu Assets → New Asset. Setelah proses pemindaian

otomatis, dashboard OSSIM menampilkan informasi lengkap seperti alamat IP, sistem operasi, dan status aktif perangkat.



Gambar 9. Hasil Scan

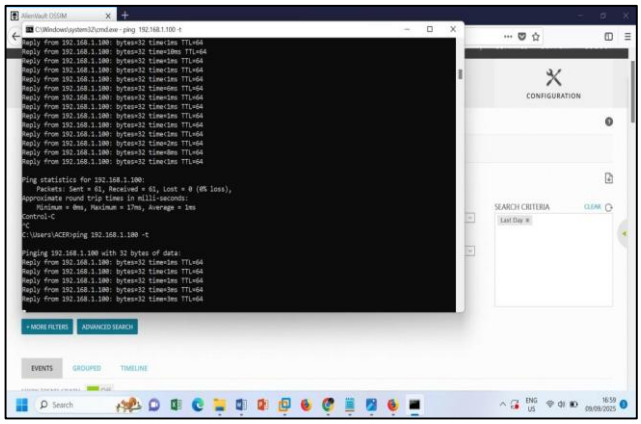
AlienVault berhasil memetakan seluruh perangkat jaringan secara otomatis dan menyimpannya dalam database aset. Fitur ini penting untuk dasar deteksi ancaman, karena setiap aktivitas jaringan dapat diidentifikasi berdasarkan aset asalnya.

Pengujian Aktivitas Jaringan (Ping Test)

Pengujian dilakukan dengan mengirimkan ICMP Echo Request (ping) dari client ke server AlienVault. Event yang dihasilkan dari aktivitas ping terekam pada log Suricata dan ditampilkan pada dashboard AlienVault. Hasil uji menunjukkan bahwa event normal dapat ditangkap dengan baik. Hal ini menjadi indikator bahwa komunikasi antar aset sudah dapat direkam dan dianalisis oleh sistem.

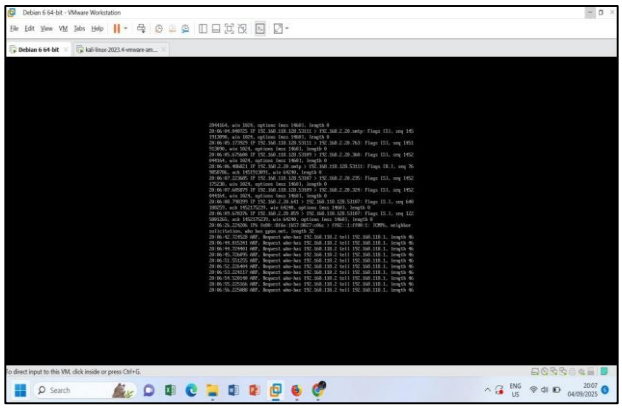
Metode yang digunakan adalah:

3. Client Windows melakukan ICMP Echo Request (ping) ke server AlienVault.



Gambar 10 Clien Melakukan Ping ke AlienVault

4. Suricata (IDS yang terintegrasi dengan OSSIM) merekam event tersebut di log Suricata.

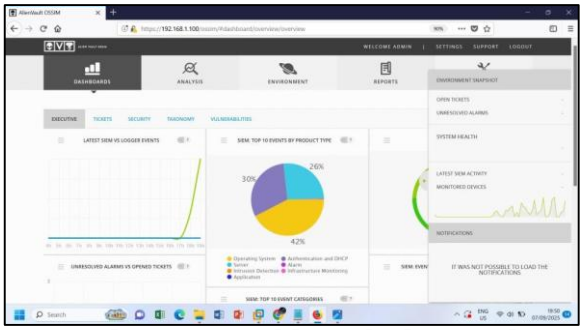


Gambar 11 Log ICMP via Console AlienVault

Suricata sebagai IDS mendeteksi lalu lintas ICMP tersebut dan mencatatnyadalam filelog di direktori/var/log/alienvault/suricata/fast.log.

Event ping kemudian diteruskan oleh OSSIM Agent ke database SIEM, dan muncul di dashboard dengan prioritas rendah (Normal Traffic).

5. Event muncul di dashboard AlienVault dengan level prioritas rendah (normal traffic).



Gambar 12. Dashboard AlienVault

Event ping berhasil ditangkap dan diklasifikasikan sebagai aktivitas jaringan normal. Hal ini membuktikan bahwa integrasi Suricata–OSSIM berjalan dengan baik, dan sistem dapat merekam aktivitas dasar jaringan secara real-time. Walaupun serangan tidak terjadi, data ICMP ini menjadi penting untuk pembentukan baseline traffic, yang nantinya digunakan oleh OSSIM dalam mendeteksi anomali atau penyimpangan pola lalu lintas di tahap monitoring selanjutnya.

Hasil uji membuktikan bahwa OSSIM dapat menangkap dan mengklasifikasikan aktivitas jaringan reguler.

Pengujian Simulasi Serangan (Port Scanning)

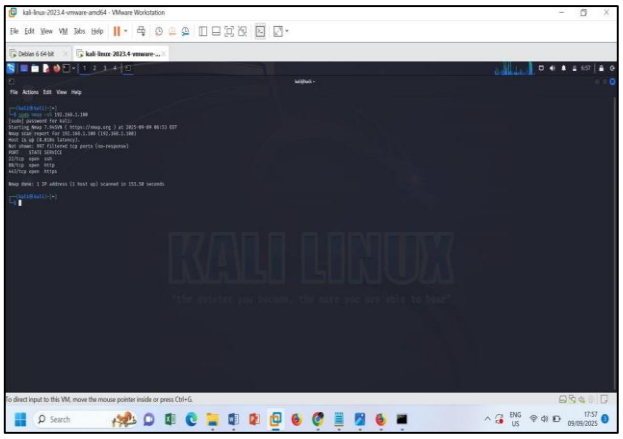
Untuk menguji kemampuan deteksi IDS, dilakukan port scanning menggunakan Nmap dari Kali Linux menuju IP AlienVault (192.168.1.100). Suricata berhasil mendeteksi

aktivitas ini sebagai event mencurigakan dan mengklasifikasikan sebagai serangan port scanning. Event tersebut muncul pada menu Analysis → Security Events di dashboard. Hasil ini menunjukkan bahwa sistem mampu membedakan aktivitas normal dan serangan.

Selama proses scanning, Suricata mendeteksi peningkatan jumlah connection attempts yang mencurigakan dan mencatatnya sebagai event dengan kategori “Attempted Information Leak” dan prioritas 2 (Medium). Event ini secara otomatis dikirim oleh ossim-agent ke server AlienVault SIEM, dan muncul pada dashboard di menu Analysis → Security Events. OSSIM menampilkan jenis event, alamat IP sumber (attacker), tujuan (victim), serta port yang diakses.

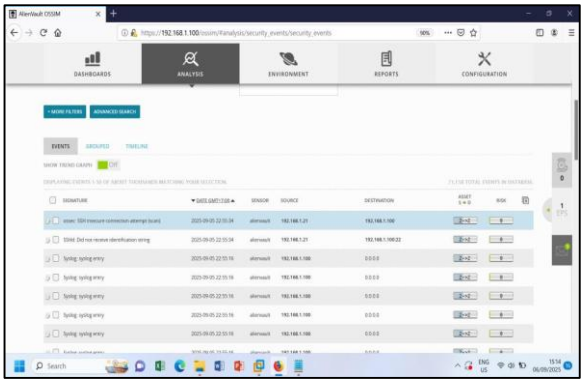
Metode yang digunakan adalah:

6. Kali Linux menjalankan tool Nmap untuk melakukan port scanning ke IP AlienVault (192.168.1.100), dengan command sudo nmap –sS 191.168.1.100



Gambar 13.Kali Linux Menjalankan Tools NMAP ke AilenVault

Suricata mendeteksi aktivitas ini sebagai event mencurigakan.



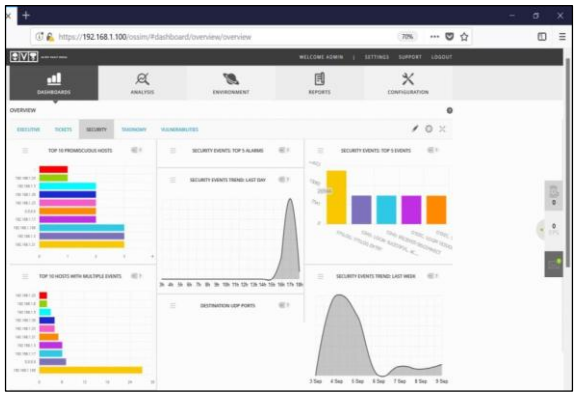
Gambar 14 Log Scanning Nmap

Sistem mendeteksi dan menampilkan aktivitas port scanning secara real-time. Alert yang dihasilkan menunjukkan bahwa mekanisme deteksi intrusi (IDS) bekerja dengan baik dan mampu membedakan antara lalu lintas normal dan aktivitas mencurigakan.

Hasil ini menunjukkan bahwa kombinasi Suricata + OSSIM tidak hanya membaca paket jaringan, tetapi juga mampu melakukan analisis kontekstual terhadap pola serangan. Aktivitas port scanning dikategorikan sebagai ancaman karena biasanya digunakan penyerang untuk memetakan port terbuka sebelum melancarkan eksploitasi lebih lanjut. Selain itu, OSSIM menyimpan semua event ini ke dalam database alienvault_siem, yang dapat digunakan untuk pembuatan laporan keamanan dan analisis forensik digital apabila terjadi insiden nyata.

7. Dashboard AlienVault menampilkan alert dengan kategori Security

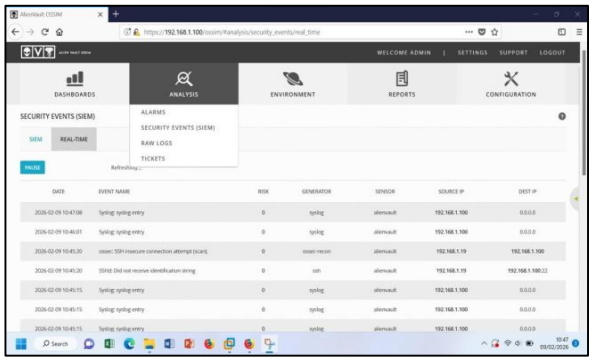
Event dan level prioritas lebih tinggi dibanding ping test.



Gambar 15. Dashbord AlienVault

Hasil ini menunjukkan bahwa sistem dapat membedakan aktivitas normal dan serangan, sekaligus menampilkan notifikasi real-time kepada administrator.

Pengujian Brute Force

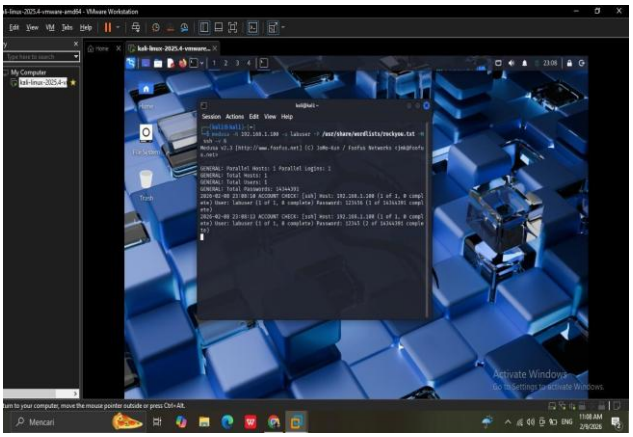


Gambar 16 Dashbord Realtime AlienVault Sebelum Diserang

Pada gambar diatas terlihat dashboard sistem keamanan AlienVault/USM pada menu Security Events (SIEM). Halaman ini menampilkan daftar aktivitas keamanan yang tercatat oleh sistem secara real-time, meliputi:

1. Tanggal dan waktu kejadian
2. Event name (jenis aktivitas)
3. Risk level (tingkat risiko)
4. Sumber (Source IP) dan tujuan (Destination IP)

Beberapa event yang muncul menunjukkan adanya aktivitas login SSH dari alamat IP tertentu menuju server internal. Aktivitas ini diberi kategori security event karena berpotensi mengindikasikan akses tidak sah atau percobaan intrusi ke dalam sistem.



Gambar 17 Pengujian Dengan Metode Brute Force

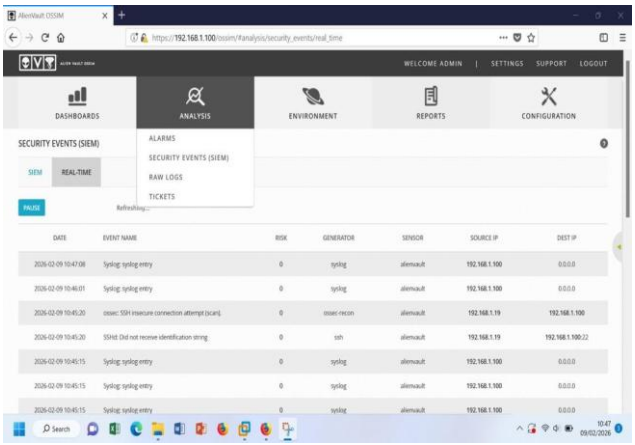
Pada gambar diatas terlihat terminal Linux yang digunakan untuk melakukan koneksi ke server melalui protokol SSH (Secure Shell).

Proses ini memperlihatkan:

a. Penggunaan perintah SSH untuk mengakses server dengan IP tujuan tertentu
b. Percobaan login menggunakan username dan password
c. Respon sistem terhadap proses autentikasi

Aktivitas ini merupakan simulasi atau pengujian akses SSH, yang dalam konteks keamanan jaringan sering digunakan untuk pengujian penetrasi (penetration testing) atau uji keamanan sistem. Setiap percobaan login, baik berhasil maupun gagal, akan dicatat oleh sistem keamanan.

Bagian	Arti
medusa	Tools untuk brute force login
-h 192.168.1.100	IP server target
-u labuser	Username yang diuji
-P rockyou.txt	Daftar password
-M ssh	Target layanan SSH
-v 6	Menampilkan detail proses



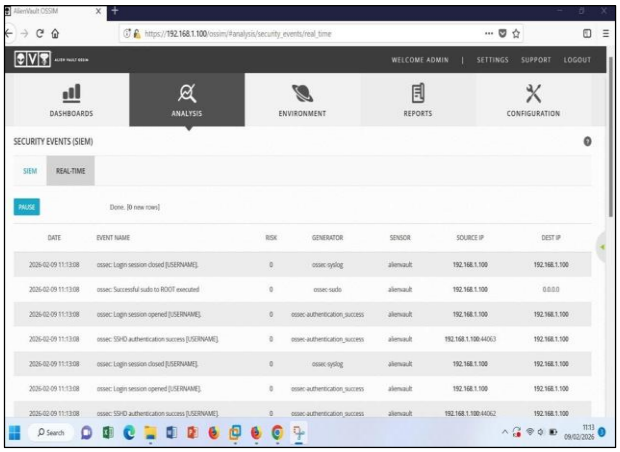
Gambar 18. Dashbord AlienVault Setelah diuji dengan Brute Force

Pada gambar diatas ditampilkan halaman Security Events Detail di AlienVault yang secara spesifik mencatat event SSH login attempt.

Informasi yang terlihat antara lain:

a. Jenis event: *SSH login attempt*
b. Status: *login*
c. Username yang digunakan
d. Alamat IP sumber dan tujuan
e. Waktu kejadian

Data ini menunjukkan bahwa sistem berhasil mendeteksi aktivitas SSH yang terjadi pada server dan mencatatnya sebagai event keamanan. Hal ini membuktikan bahwa sistem monitoring bekerja dengan baik dalam memantau akses jarak jauh.



Gambar 19. Dashbord Alienvault Setelah Diuji Dengan Brute Force

Pada gambar diatas terlihat rekap beberapa event SSH yang terjadi secara berulang dalam rentang waktu tertentu.

Beberapa event memiliki pola yang sama, seperti:
1. Percobaan login SSH berulang
2. Penggunaan akun tertentu
3. Sumber IP yang sama

Pola ini dapat dianalisis lebih lanjut sebagai:
1. Percobaan brute force
2. Uji penetrasi terkontrol
3. Atau aktivitas mencurigakan yang berpotensi menjadi ancaman keamanan

AlienVault mengelompokkan dan menampilkan event-event tersebut sehingga memudahkan administrator dalam melakukan analisis dan pengambilan keputusan.

B.Pembahasan

Berdasarkan hasil pengujian, sistem AlienVault OSSIM mampu melakukan monitoring aktivitas jaringan serta mendeteksi adanya serangan sederhana seperti port scanning. Penerapan metode Network Development Life Cycle (NDLC) pada penelitian ini terbukti efektif untuk membangun sistem monitoring dan keamanan jaringan secara terstruktur:

Dalam penelitian ini, digunakan metode Network Development Life Cycle (NDLC) untuk mendukung alur kerja yang lebih sistematis. Pada tahap analisis, permasalahan utama yang ditemukan adalah ketiadaan sistem monitoring dan keamanan terintegrasi di SMK N 4 Bengkulu. Selanjutnya, tahap desain dilakukan dengan merancang topologi jaringan interkoneksi yang mampu mengakomodasi kebutuhan monitoring. Tahap simulation prototyping dilaksanakan dengan membuat model jaringan virtual menggunakan VMware, yang kemudian direalisasikan pada tahap implementasi dengan menginstal dan mengonfigurasi AlienVault OSSIM.

1. Analysis: dilakukan analisis kebutuhan jaringan dan identifikasi permasalahan.
2. Design: merancang topologi jaringan interkoneksi yang sesuai kebutuhan SMK N 4 Bengkulu.
3. Simulation Prototyping: membangun prototipe sistem menggunakan VMware dan tools grafis.
4. Implementation: menginstal dan mengonfigurasi AlienVault OSSIM sebagai IDS/IPS.
5. Monitoring: melakukan pengawasan melalui dashboard AlienVault terhadap traffic jaringan.
6. Management: merumuskan kebijakan agar sistem keamanan dapat berjalan berkesinambungan.

Tahap monitoring dilakukan dengan mengamati event melalui dashboard OSSIM, baik untuk lalu lintas normal maupun anomali. Hasilnya, OSSIM dapat menampilkan event ping dengan prioritas rendah dan port scanning dengan prioritas tinggi. Tahap terakhir, management, berfokus pada pentingnya kebijakan keamanan jaringan agar sistem dapat berjalan secara berkesinambungan, misalnya melalui pembaruan signature IDS, pengaturan kebijakan akses internet, serta pengelolaan aset jaringan secara terpusat.

Interpretasi Hasil

a. Ping Test → dianggap sebagai traffic normal dengan prioritas rendah.
b. Port Scanning → dikategorikan sebagai ancaman dengan prioritas lebih tinggi.
c. Brute Force Attack → terdeteksi sebagai percobaan akses tidak sah dengan prioritas tinggi.

Hasil ini menegaskan bahwa OSSIM tidak hanya menyimpan log, tetapi juga menganalisis pola serangan secara kontekstual.

Dari keseluruhan tahapan ini, dapat dilihat bahwa OSSIM bukan hanya sekadar mencatat log, melainkan juga melakukan analisis terhadap pola serangan. Dengan demikian, sistem ini dapat menjadi solusi tepat untuk meningkatkan keamanan jaringan di SMK N 4 Bengkulu.

C.Hasil Pengujian

Hasil pengujian menunjukkan bahwa AlienVault OSSIM mampu merekam aktivitas jaringan, baik berupa traffic normal maupun serangan. Pada pengujian ping flooding (ICMP flood), event terekam sebagai aktivitas jaringan dengan tingkat prioritas rendah hingga sedang. Pada pengujian port scanning, sistem IDS Suricata yang terintegrasi dalam OSSIM mampu mendeteksi aktivitas pemindaian port dan mengklasifikasikannya sebagai ancaman keamanan. Selain itu, pada pengujian brute force menggunakan Medusa terhadap layanan SSH, OSSIM berhasil mendeteksi percobaan login berulang yang mencurigakan dan mencatatnya sebagai security alert.

Dashboard OSSIM juga berhasil menampilkan ringkasan event secara real- time, sehingga administrator jaringan dapat dengan mudah memantau kondisi keamanan jaringan yang sedang berlangsung.

 P-ISSN 1858-2680
E-ISSN 2723-4673

Secara keseluruhan, hasil pengujian dapat dirangkum sebagai berikut::

1. AlienVault OSSIM berhasil menampilkan aktivitas jaringan normal maupun anomali, termasuk ping flooding, pada dashboard sistem.
2. Suricata mampu mendeteksi serangan portscanning dan mengklasifikasikan sebagai peringatan keamanan (security alert).
3. Sistem OSSIM berhasil mendeteksi percobaan brute force pada layanan SSH sebagai bentuk akses tidak sah.
4. Dashboard AlienVault mampu memberikan visualisasi real-time terhadap seluruh event yang terjadi di jaringan.

V. PENUTUP

A.Kesimpulan

Berdasarkan hasil implementasi dan pengujian AlienVault OSSIM pada jaringan virtual di SMK N 4 Bengkulu, dapat disimpulkan bahwa sistem ini berhasil diinstal dan dijalankan dengan baik menggunakan VMware dengan konfigurasi interface eth0 sebagai manajemen dan eth1 sebagai monitoring. Sistem mampu melakukan monitoring terhadap aset jaringan yang ditambahkan serta berhasil mendeteksi aktivitas normal berupa ping maupun aktivitas berbahaya berupa port scanning.

Penggunaan metode NDLC dalam penelitian ini terbukti mendukung proses pembangunan sistem secara terstruktur, mulai dari tahap analisis kebutuhan hingga tahap manajemen kebijakan. Dengan demikian, AlienVault OSSIM terbukti mampu menjadi solusi monitoring dan keamanan jaringan yang efektif, terutama untuk lingkungan sekolah yang membutuhkan pengawasan ketat terhadap lalu lintas data.

Hasil implementasi dan pengujian AlienVault OSSIM pada jaringan virtual di SMK N 4 Bengkulu, maka dapat disimpulkan bahwa:

1. AlienVault OSSIM berhasil diinstal dan dijalankan pada VMware dengan konfigurasi interface eth0 sebagai manajemen dan eth1 sebagai monitoring.
2. Sistem mampu melakukan monitoring terhadap aset jaringan yang ditambahkan.
3. AlienVault OSSIM berhasil mendeteksi aktivitas normal (ping) maupun serangan sederhana (port scanning) melalui integrasi dengan Suricata.
4. Metode NDLC terbukti mendukung penerapan sistem keamanan jaringan yang lebih terstruktur dan terarah.

B. Saran

Untuk pengembangan lebih lanjut, penelitian ini masih dapat disempurnakan. Pengujian dapat diperluas dengan mencoba serangan yang lebih kompleks seperti SQL Injection atau Denial of Service (DoS) untuk menguji ketahanan sistem. Selain itu, AlienVault OSSIM dapat diintegrasikan dengan perangkat keamanan lain seperti firewall eksternal agar sistem pertahanan jaringan lebih komprehensif. Dari sisi visualisasi, dashboard dapat ditingkatkan dengan tampilan yang lebih interaktif agar administrator lebih mudah memahami situasi keamanan secara real-time. Terakhir, dibutuhkan kebijakan keamanan yang konsisten agar sistem tetap efektif dalam jangka panjang dan mampu menjaga reliabilitas jaringan.

Saran untuk penelitian selanjutnya adalah:

1. Melakukan pengujian dengan serangan yang lebih kompleks, seperti SQL Injection atau DoS.
2. Mengintegrasikan AlienVault OSSIM dengan perangkat keamanan lain seperti firewall eksternal.
3. Mengembangkan dashboard dengan visualisasi tambahan agar lebih mudah dipahami oleh administrator jaringan.
4. Menerapkan kebijakan keamanan jaringan secara konsisten agar sistem tetap efektif dalam jangka panjang.

DAFTAR PUSTAKA

[1] Abdullah, Bobby. 2020. *Analisis Kerentanan Menggunakan Alienvault Dan Qualys Pada Security Operation Center (SOC) Berdasarkan Framework Cyber Kill*. e-Proceeding of Engineering. Fakultas Rekayasa Industri, Universitas Telkom

[2] Al amin, Muh. 2024. *Implementasi Security Information And Event Management (SIEM) Dalam Meningkatkan Keamanan Jaringan*. JURTIKOM – Jurnal Riset Teknik Komputer. Institut Teknologi Bacharuddin Jususf Habibie, Parepare Sulawesi Selatan

[3] Anugrah, Rio Wahyudin. 2024. *Transformasi Sosial : Perubahan Kehidupan Masyarakat Melalui Penyebaran Jaringan Komputer*. ADIMAS – Adi Pengabdian Kepada Masyarakat. Universitas Raharja

[4] Ariadi, Fadly. 2024. *Pengenalan Model 7 Osi Layer Pada Siswa-Siswi Sma Islam Terpadu Insan Madani 8*. Praxis – Jurnal Pengabdian Kepada Masyarakat. Teknik informatika, Ilmu Komputer, Universitas Pamulang

[5] Hanifah, Fatin. 2021. *Analisa Kerentanan Pada Vulnerable Docker Menggunakan Alienvault Dan Docker Bench For Security Dengan Acuan*

 P-ISSN 1858-2680
E-ISSN 2723-4673

Framework Cis Control. e-Proceeding of Engineering. Universitas Telkom, Bandung

[6] Khairunnisa, Puteri Ananda. 2024. *Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia*. Teknik: Jurnal Ilmu Teknik dan Informatika. Universitas Palangka Raya

[7] Khotimah, Husnul. 2022. *Implementasi Security Information And Event Management (SIEM) Pada Aplikasi SMS Center Pemerintah Daerah Provinsi Nusa Tenggara Barat.* JbegaTI. Dinas Komunikasi Informatika dan Statistik Pemerintah Provinsi Nusa Tenggara Barat

[8] Purnomo, Andi. 2024. *Peran Artificial Intelligence dalam Deteksi Dini Ancaman Keamanan Jaringan*. Jurnal Minfo Polgan. Universitas Ary Ginanjar

[9] Ramadhani, Shafwan Iman. 2024. *Penerapan Komunikasi Data Pada Osi Layer PC to PC Menggunakan Cisco Packet Tracer*. Jurnal Penelitian Rumpun Ilmu Teknik (JUPRIT). Universitas Sultan Ageng Tirtayasa[10] Saputra, Ganda. 2024. *Sosialisasi Pengenalan Komputer Dan Perangkat Komputerdesa Dalihan Natolu*. Jurnal Penyuluhan dan Pemberdayaan Masyarakat (JPPM). Fakultas Ekonomi dan Bisnis, Prodi Akuntansi, Universitas Labuhanbatu

[11] Trianto, Nanang. 2020. *Implementasi Indicator of Compromise OTX AlienVault pada MISP Threat Sharing untuk Network Intrusion Detection System Suricata*. JATI (Jurnal Mahasiswa Teknik Informatika). Politeknik Siber dan Sandi Negara

[12] Wilujeng, Cahya Kamila. *Implementasi Firewall Filter Rules Sebagai Filtering Content Pada Jaringan Komputer Menggunakan Mikrotik*. JATI (Jurnal Mahasiswa Teknik Informatika). Sistem Informasi, Universitas Singaperbangsa Karawang

 P-ISSN 1858-2680
E-ISSN 2723-4673