Jurnal Ilmu Komputer dan Sistem Informasi (JIKSI)

Vol. 11, No. 8, Agustus 2025, hlm. 19-32

PENERAPAN SISTEM KEAMANAN JARINGAN MENGGUNAKAN INTRUSION PREVENTION SYSTEM (IPS) BERBASIS SURICATA PADA KANTOR CAMAT LAMASI TIMUR

Chairunnisa[1], Siaulhak[2], Ichwan Muis[3]
chairunnisanisa068@gmail.com[1], siaulhak@uncp.ac.id[2], ichwanmuis@gmail.com[3]
Universitas Cokroaminoto Palopo

Abstrak

Penelitian ini bertujuan untuk menerapkan sistem keamanan jaringan di Kantor Camat Lamasi Timur melalui penerapan sistem keamanan jaringan menggunakan intrusion prevention system (IPS) berbasis suricata. Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif untuk mengidentifikasi serangan. Serangan siber seperti ICMP ping menjadi ancaman serius karena dapat melumpuhkan jaringan dan mengganggu proses pembelajaran. Suricata, sebagai sistem intrusion prevention system (IPS), berperan dalam melaksanakan deteksi serta pencegahan serangan dengan memeriksa paket data secara realtime. Namun, pengelolaan keamanan yang masih manual menjadi tantangan, terutama saat serangan menghambat akses jarak jauh untuk perbaikan. Penelitian ini bertujuan mengimplementasikan suricata sebagai intrusion prevention system (IPS) untuk secara proaktif mencegah serangan, menggabungkan pemblokiran IPTables dengan inspeksi mendalam dari intrusion prevention system (IPS). Dengan solusi ini, Kantor Camat Lamasi Timur diharapkan dapat mengurangi intervensi manual, meningkatkan keamanan data, dan memastikan stabilitas jaringan. Implementasi suricata sebagai intrusion prevention system (IPS) menjadi langkah strategis untuk melindungi kantor dari serangan ICMP ping dan mendukung proses administrasi yang aman.

Kata Kunci: Keamanan Jaringan; IPS, Suricata; ICMP Ping.

1. PENDAHULUAN

Perkembangan teknologi informasi merupakan bukti bahwa manusia terus berinovasi dalam menghadapi tantangan dan mencari cara untuk mengatasinya, sehingga solusi yang ditemukan dapat menjadi dasar untuk menciptakan ide-ide baru yang mendukung kemajuan teknologi informasi demi kemudahan dalam kehidupan masyarakat. Namun, seiring dengan kemajuan tersebut, muncul pula dampak negatif, salah satunya masalah keamanan. Saat ini, serangan siber menargetkan individu, bisnis, organisasi pemerintah, dan lainnya. Serangan-serangan ini bertujuan untuk merusak integritas sistem, mencuri informasi, dan dalam beberapa kasus, menyebabkan kerusakan pada sistem yang membuatnya tidak dapat digunakan (Rivaldi & Marpaung, 2023). Sistem keamanan jaringan adalah upaya untuk mencegah dan mengidentifikasi pengguna jaringan yang tidak sah (penyusup) dalam suatu jaringan. Langkah pencegahan ini bertujuan untuk menghentikan akses pengguna yang tidak sah terhadap berbagai elemen dalam jaringan yang telah mereka masuki. Sistem keamanan jaringan berperan penting dalam menjaga stabilitas jaringan dan memastikan efektivitas penggunaan data pengguna (Rivaldi & Marpaung, 2023).

Intrusion prevention system (IPS) adalah sebuah sistem yang menggabungkan fungsi firewall dan fungsi IDS dengan proporsional. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, disaat serangan telah teridentifikasi, IPS akan menolak akses

(block) dan mencatat (log) semua paket data yang teridentifikasi tersebut (Anggoro, 2019). Suricata merupakan IDS, IPS, dan alat monitoring keamanan jaringan yang berbasis open-source. Suricata adalah sebuah tool keamanan jaringan dengan performa tinggi yang memiliki kemampuan multi-threaded. Suricata mampu mendeteksi gangguan secara real-time, pencegahan intrusi inline (IPS), pemantauan keamanan jaringan (NSM), dan pemrosesan PCAP offline (Anugrah, 2022).

Berdasarkan hasil observasi atau pengamatan yang dilakukan pada Kantor Camat Lamasi Timur yang beralamat di JL. Poros To'lemo, Kecamatan Lamasi Timur, Kabupaten Luwu. Di dalam jaringan Kantor Camat Lamasi Timur, banyak aktivitas yang terkait dengan jaringan, termasuk untuk mendukung berbagai kegiatan administrasi dan pelayanan publik. Dengan semakin meningkatnya ancaman siber, terutama serangan yang dapat merusak integritas data dan merusak jaringan internal. Namun, saat ini belum ada sistem pendeteksi serangan seperti IPS. Kantor Camat Lamasi Timur saat ini hanya mengandalkan sistem keamanan dasar (firewall dan antivirus) tanpa adanya pemantauan lanjutan terhadap ancaman di dalam jaringan yang lebih kompleks. Tanpa adanya intrusion prevention system (IPS), potensi serangan yang masuk ke jaringan bisa terjadi tanpa terdeteksi. Oleh karena itu, dibutuhkan sebuah sistem pencegahan serangan yang mampu memberikan peringatan saat terjadi penyusupan data atau paket yang bersifat berbahaya di jaringan Kantor Camat Lamasi Timur.

Adapun solusi yang ditawarkan dari permasalahan mengenai keamanan jaringan yang ada di Kantor Camat Lamasi Timur yaitu perlu adanya "penerapan sistem keamanan jaringan menggunakan intrusion prevention system (IPS) berbasis suricata" merupakan langkah strategis untuk memperkuat keamanan jaringan di Kantor Camat Lamasi Timur. Suricata yang merupakan sistem open-source, dapat menganalisis lalu lintas jaringan secara real-time, mendeteksi intrusi, dan memberikan perlindungan aktif terhadap potensi serangan. Dengan kemampuannya dalam menangani berbagai protokol dan jenis lalu lintas, suricata dapat membantu mengidentifikasi dan mencegah ancaman sebelum menyebabkan kerusakan pada sistem. Dengan penerapan suricata, diharapkan Kantor Camat Lamasi Timur dapat meningkatkan keamanan data, melindungi informasi sensitif, dan memastikan kelancaran pelayanan publik. Selain itu, sistem ini juga dapat menyediakan laporan dan analisis mengenai potensi ancaman yang berguna untuk pengambilan keputusan terkait kebijakan keamanan.

Atas terjadinya permasalahan tersebut untuk memperkuat argumen, maka penulis mengambil topik penelitian tentang keamanan jaringan dengan judul penelitian "Penerapan sistem keamanan jaringan menggunakan intrusion prevention system (IPS) berbasis suricata pada Kantor Camat Lamasi Timur", di harapkan dapat mengimplementasikan intrusion prevention system (IPS), di mana sistem IPS yang memanfaatkan firewall dapat mendeteksi serangan berbasis port dan protokol, menolak akses, serta mencatat log yang teridentifikasi sebagai ancaman. Penelitian ini juga diharapkan dapat menjadi referensi untuk penerapan sistem keamanan jaringan berbasis suricata yang lebih maju di masa depan.

2. METODE PENELITIAN

Pada penelitian ini, penulis menggunakan jenis penelitian kualitatif yang merupakan sebuah penelitian yang menekankan pada aspek pemahaman lebih mendalam terhadap suatu masalah daripada melihat sebuah permasalahan. Menurut Sugiyono, menyatakan bahwa metode penelitian kualitatif berlandaskan filasafat positivisme dan berfokus pada kondisi obyek alami. Hasilnya lebih signifikan daripada generalisasi (Haryono, 2023). Dalam melakukan penelitian ini, peneliti

menggunakan metode intrusion prevention system dengan menggunakan suricata sebagai metodologi penelitian. Intrusion prevention system (IPS) berbasis suricata merupakan prosedur yang digunakan untuk melakukan penelitian tentang keamanan jaringan dengan melakukan pencegahan terhadap serangan yang ketat dengan menerapkan aturan dari suricata yang tepat untuk mengatasi setiap serangan. Metodologi penelitian ini bertujuan untuk mendapatkan pemahaman yang mendalam tentang bagaimana proses implementasi, tantangan, dan dampaknya secara detail berdasarkan pengalaman nyata di lapangan. Dengan pendekatan yang tepat, penelitian ini dapat memberikan wawasan berharga untuk meningkatkan keamanan jaringan di Kantor Camat Lamasi Timur.

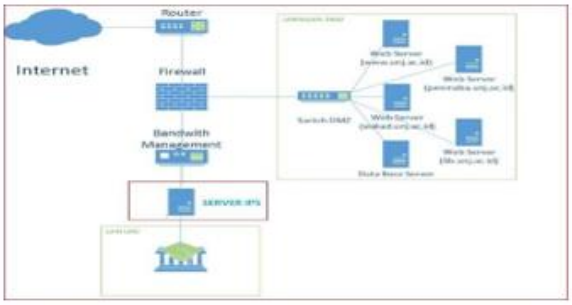
3. HASIL DAN PEMBAHASAN

Hasil penelitian merupakan tahap dimana penerapan sistem keamanan jaringan menggunakan intrusion prevention system (IPS) berbasis suricata pada Kantor Camat Lamasi Timur yang sudah penulis terapkan dapat dipaparkan. Hasil dari penerapan sistem keamanan jaringan menggunakan intrusion prevention system (IPS) berbasis suricata ini dapat kita ketahui apakah keamanan jaringan yang di terapkan dapat digunakan sebagai sistem keamanan jaringan yang baru dan mengamankan jaringan Kantor Camat Lamasi Timur.

1. Perancangan Sistem Keamanan

Perancangan Sistem Keamanan adalah proses merancang dan megimplementasikan langkah-langkah untuk melindungi sumber daya dan informasi dari ancaman atau serangan. Sistem ini harus dirancang untuk mencegah, mendeteksi, dan merespons ancaman yang dapat membahayakan integritas, kerahasian, dan ketersediaan data atau aset.

Skema jaringan yang dipakai dalam penempatan server intrusion prevention system (IPS) penelitian ini dapat dilihat pada gambar 21.



Gambar 1. Penempatan *Server* IPS
Sumber: Hasil Tangkapan Layar Penulis (2025)

Pada Gambar 1, desain jaringan baru yang dirancang pada dasarnya sama dengan jaringan yang sudah ada tetapi, pada jaringan yang baru ditambahkan penggunaan server intrusion prevention systen (IPS) baru diatas jaringan server lokal Kantor Camat sebagai alat filtering paket yang keluar dari internet yang disediakan Kantor Camat.

Implementasi Sistem

1. Instalasi dan Konfigurasi Suricata

Instalasi dilakukan pada sistem operasi Ubuntu 20.04 menggunakan VirtualBox. Suricata dipasang dan dikonfigurasi untuk memantau lalu lintas jaringan. File konfigurasi suricata.yaml disesuaikan dengan interface jaringan yang aktif agar dapat menangkap semua lalu lintas data masuk dan keluar.

Suricata kemudian dihubungkan dengan file rules (aturan) yang digunakan untuk mendeteksi berbagai jenis serangan, seperti:

a. Port scanning
b. Ping of Death
c. SYN Flood
d. SQL Injection

2. Integrasi dengan IPTables

Suricata diintegrasikan dengan iptables untuk melakukan tindakan pencegahan secara otomatis (blocking) terhadap lalu lintas jaringan yang mencurigakan. Dengan skenario serangan yang disimulasikan menggunakan hping3 dari Kali Linux, sistem dapat:

a. Mendeteksi dan memblokir IP penyerang
b. Mencatat log serangan di

/var/log/suricata/

3. Instalasi Suricata

Tahapan pertama yaitu menambahkan repository dari Suricata dengan command sudo add-apt- repository ppa:oisf/Suricata-stable, Gambar menambahkan repository dapat dilihat pada Gambar 22.

Gambar 2. Menambahkan *Repository Suricata*
Sumber: Hasil Tangkapan Layar Penulis (2025)

Gambar 2. menampilkan proses awal dalam instalasi suricata, yaitu penambahan repository resmi suricata ke dalam sistem operasi Ubuntu. Repository adalah sumber resmi tempat paket-paket perangkat lunak disimpan, dan menambahkannya memungkinkan sistem untuk mengunduh dan memperbarui Suricata secara otomatis dari sumber terpercaya.

Tahapan selanjutnya instalasi suricata dengan command dan sudo apt- get install Suricata, instalasi suricata dapat dilihat pada Gambar 3.

Gambar 3. Instalasi *Suricata*
Sumber: Hasil Tangkapan Layar Penulis (2025)

Gambar 3. menunjukkan proses instalasi suricata pada sistem operasi Ubuntu 20.04 setelah repository resmi berhasil ditambahkan (seperti yang dijelaskan pada Gambar 23).

Gambar ini mendokumentasikan tahapan teknis penting dalam proses implementasi sistem keamanan jaringan, yaitu pemasangan aplikasi inti (suricata). Ini menunjukkan bahwa perangkat lunak berhasil dipasang secara lokal dan siap untuk dikonfigurasi sesuai kebutuhan jaringan di Kantor Camat Lamasi Timur.

Langkah berikutnya mengecek status suricata, suricata akan langsung aktif setelah di install. Unuk tahapan enable dan melihat suricata sudah aktif bisa dilakukan dengan command sudo systemctl enable suricata dan sudo systemctl status suricata.service dapat dilihat pada gambar berikut.

Gambar 4. Pengecekan Status *Suricata*
Sumber: Hasil Tangkapan Layar Penulis (2025)

Gambar ini menjadi bukti bahwa implementasi Suricata telah berhasil hingga tahap eksekusi, bukan hanya sekadar instalasi. Ini menandakan bahwa sistem keamanan jaringan sudah siap untuk memantau, mencatat, dan merespons lalu lintas jaringan secara real-time di lingkungan Kantor Camat Lamasi Timur.

Informasi yang Ditampilkan di Gambar.

Status layanan ditampilkan dalam bentuk informasi log seperti:

a. Active (running): menunjukkan bahwa suricata sedang berjalan dengan normal.
b. Loaded: menunjukkan bahwa layanan telah berhasil dimuat oleh sistem.
c. Main PID: nomor identifikasi proses suricata yang sedang aktif.
d. Log terakhir: baris-baris log terakhir menunjukkan aktivitas atau error jika ada.

Gambar 5. Konfigurasi *Suricata*
Sumber: Hasil Tangkapan Layar Penulis (2025)

Gambar 5. merupakan konfigurasi IP Address komputer yang ingin dimonitoring. Pengeditan konfigurasi dari Suricata dapat dilakukan dengan command sudo nano /etc/suricata/suricata.yaml.

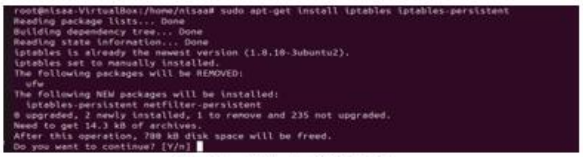
Isi Konfigurasi (Yang Umumnya Disesuaikan)

Dalam file ini, konfigurasi penting yang diubah antara lain:

a. Interface jaringan (interface: eth0 atau sesuai nama interface aktif), agar Suricata tahu dari mana lalu lintas jaringan akan dimonitor.
b. File log: menentukan lokasi dan format penyimpanan hasil deteksi serangan.
c. Rules-path: mengarahkan suricata ke folder tempat aturan (rules) disimpan.
d. Detection-engine: mengatur parameter deteksi serangan (seperti depth, search-

method).

4. Instalasi IpTables



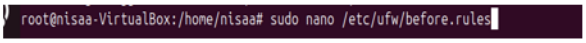
Gambar 6. Install IPTables
Sumber: Hasil Tangkapan Layar Penulis (2025)

Gambar 6. merupakan langkah berikutnya dengan menginstall IPTables, dengan command sudo apt-get install iptables iptables-persistent.

Gambar ini menunjukkan bahwa sistem telah dilengkapi dengan firewall aktif dan dapat disesuaikan untuk bekerja bersama Suricata. IPTables akan memungkinkan sistem tidak hanya mendeteksi serangan, tetapi juga mengambil tindakan tegas seperti memblokir IP penyerang. Langkah ini merupakan bagian krusial dalam membangun intrusion prevention system (IPS) berbasis suricata yang responsif dan otomatis.

Fungsi IPTables:

a. Menentukan aturan (rules) yang mengizinkan, menolak, atau memblokir trafik jaringan berdasarkan IP, port, atau protokol.
b. Bekerja bersama suricata untuk menjalankan tindakan pencegahan secara otomatis terhadap paket data yang mencurigakan.
c. Meningkatkan keamanan jaringan dengan memberikan perlindungan lapis kedua setelah pendeteksian oleh suricata.



Gambar 7. Konfigurasi *IPTables*
Sumber: Hasil Tangkapan Layar Penulis (2025)

Gambar 7. merupakan tahapan konfigurasi rules yang ingin diterapkan di IPTables dengan command sudo nano /etc/ufw/before.rules.

Gambar ini menunjukkan proses penting dalam membangun sistem intrusion prevention system (IPS) berbasis suricata yang sepenuhnya otomatis dan responsif. Konfigurasi before rules memberikan dasar bagi sistem untuk:

a. Memutus koneksi mencurigakan
b. Melindungi port penting
c. Mencegah akses tidak sah

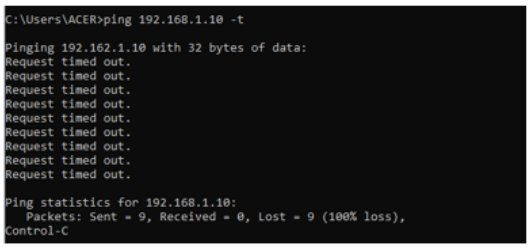
Ini memastikan bahwa sistem keamanan jaringan di Kantor Camat Lamasi Timur tidak hanya mendeteksi, tetapi juga secara aktif melindungi infrastruktur dari berbagai serangan siber.

Evaluasi Sistem

Pengujian Sistem Keamanan Jaringan merupakan proses untuk mengevaluasi efektivitas Sistem Keamanan Jaringan dalam mencegah, mendeteksi, dan merespons serangan. Tujuan pengujian ini merupakan untuk menentukan apakah sistem keamanan jaringan dapat mencegah serangan yang dicobakan. Penelitian ini melakukan pengujian untuk mengambil data dengan skenario serangan yang sudah dilakukan untuk mengetahui kinerja dari Suricata dan IPTables. Pengambilan Data dilakukan oleh peneliti dengan melakukan pengamatan secara langsung dari log suricata pada saat terjadi serangan ICMP ping.

a. Skenario Pertama dan Hasil

Dalam Skenario Pertama ini serangan yang dilakukan berupa satu laptop penyerang akan melakukan serangan dengan jenis serangan ICMP ping yang dapat dilihat pada Gambar 8.



Gambar 8. Uji Coba
Sumber: Hasil Tangkapan Layar Penulis (2025)

1) Simulasi Serangan
   a) Uji coba dilakukan menggunakan perangkat laptop penyerang yang mengirimkan serangan ICMP ping secara berulang ke target (komputer dalam jaringan lokal).
   b) Serangan ini biasa digunakan untuk

melakukan ping flood atau denial of service (DoS) ringan, dan juga untuk memetakan jaringan melalui scanning.

2) Tujuan Pengujian
   a) Untuk menguji apakah suricata mampu mendeteksi lalu lintas ICMP yang mencurigakan.
   b) Untuk memverifikasi apakah IPS akan memblokir paket serangan secara otomatis.
3) Respons Sistem
   a) Berdasarkan gambar, suricata memberikan alert secara real-time yang mengidentifikasi serangan ICMP.
   b) Sistem mencatat peringatan ke log dan melakukan pemblokiran (drop) terhadap paket dari IP penyerang.
   c) Waktu serangan yang tercatat di log sesuai dengan waktu percobaan serangan, menunjukkan bahwa sistem berfungsi secara live monitoring.
4) Hasil
   a) Serangan berhasil diblokir oleh sistem IPS, membuktikan bahwa konfigurasi Suricata dan IPTables berjalan sesuai harapan.
   b) Gambar ini menunjukkan bukti konkret bahwa sistem tidak hanya mendeteksi tetapi juga mencegah serangan dari mencapai targetnya.

Intrusion prevention system (IPS) memberikan alert serta melakukan drop paket yang dilakukan penyerang, untuk memastikan suricata bekerja secara real time. Tampak waktu yang di tampilan di log suricata sama dengan waktu penyerangan dan IPS telah berhasil mencegah serangan ICMP ping.

Gambar 9. *Log* Serangan ICMP *Ping*
Sumber: Hasil Tangkapan Layar Penulis (2025)

Berdasarkan Gambar 9. yang telah dilakukan yaitu instalasi suricata dan IPTables telah berhasil dilakukan dan berjalan sesuai konfigurasi telah kita lakukan. Adapun sistem pencegahan serangan intrusion prevention system (IPS) dapat memberikan pemberitahuan serangan dan mencegah serangan terjadi. Pola serangan yang ada dalam aturan IPS menyebabkan serangan terdeteksi, sehingga perangkat IPS harus dikonfigurasi dengan benar dan sering mengembangkan aturan IPS. Hasil dari yang telah dilakukan percobaan dapat dilihat pada Gambar 9.

Gambar ini menampilkan hasil log yang dihasilkan oleh suricata saat terjadi serangan pada jaringan dalam hal ini adalah serangan ICMP ping yang dilakukan dari perangkat penyerang.

Komponen Penting dalam Gambar 9:

1. Timestamp (Waktu Serangan)

Log menunjukkan waktu kejadian serangan secara real-time, memberikan informasi kapan tepatnya serangan terjadi. Ini penting untuk keperluan forensik dan pelacakan insiden.

2. Source IP dan destination IP

Informasi mengenai IP sumber serangan (IP penyerang) dan IP tujuan (komputer target dalam jaringan Kantor Camat Lamasi Timur). Hal ini memudahkan administrator dalam mengidentifikasi asal serangan.

3. Jenis Serangan

Suricata mencatat jenis serangan yang terdeteksi, dalam hal ini adalah:

a. "ICMP Ping" yang menunjukkan adanya upaya melakukan ping flood atau probing untuk mencari kerentanan.
b. Action baris log menunjukkan bahwa sistem "dropped" paket serangan, artinya suricata bekerja sama dengan IPTables telah memblokir serangan sebelum mencapai sistem target.
c. Rule signature log juga menyebutkan signature ID (SID) dari aturan yang dikenali. Ini menandakan bahwa serangan tersebut cocok dengan salah satu aturan (rules) yang telah diaktifkan di file konfigurasi suricata.

b. Skenario Kedua dan Hasil

Dalam Skenario Kedua ini serangan yang dilakukan berupa satu laptop penyerang akan melakukan serangan dengan jenis serangan Port Scanning.

Gambar 10. *Log* Serangan *Port Scannning*
Sumber: Hasil Tangkapan Layar Penulis (2025)

Berdasarkan gambar diatas, serangan port scanning ini dilakukan oleh perangkat penyerang dengan IP sumber 192.168.1.1 dan port 15919, yang mencoba mengakses beberapa IP tujuan dalam jaringan menggunakan protokol TCP. Berdasarkan log, serangan terdeteksi pada tanggal 14 juni 2025 pukul 10:30:20, dan langsung diklasifikasikan sebagai ancaman dengan prioritas tingkat 3 (medium). Sistem suricata secara otomatis melakukan aksi pencegahan dengan men-drop paket mencurigakan, ditandai dengan status "[Drop]" dalam log. Serangan port scanning merupakan metode umum untuk memetakan port terbuka pada sistem target, yang berpotensi dimanfaatkan untuk eksploitasi lebih lanjut. Dengan keberhasilan sistem dalam mendeteksi dan memblokir serangan ini, dapat disimpulkan bahwa IPS berbasis suricata memberikan perlindungan aktif yang efektif terhadap anacaman keamanan jaringan di lingkungan Kantor Camat Lamasi Timur.

c. Skenario Ketiga dan Hasil

Gambar 11. *Log* Serangan HTTP *Flood*
Sumber: Hasil Tangkapan Layar Penulis (2025)

Serangan ini pada tanggal 24 juni 2025 sekitar pukul 12:08 hingga 12:15, dengan IP sumber 192.168.1.10 yang secara terus-menerus mengirim permintaan HTTP menuju IP target 192.168.1.1 pada port 80, yaitu port layanan web. Dalam log, suricata mendeteksi pola lalu lintas yang tidak normal dan mengidentifikasinya sebagai "HTTP flood attack detected", yang tergolong dalam klasifikasi attemped denial of service (DoS) dengan priotas ancaman tingkat 2. Serangan jenis ini bertujuan membanjiri server web dengan permintaan berlebihan sehingga menyebabkan gangguan layanan. Sistem secara otomatis mengambil tindakan pencegahan dengan men-drop setiap paket mencurigakan, yang ditandai dengan status "[Drop]" pada log. Deteksi yang cepat dan akurat ini membuktikan bahwa penerapan suricata efektif dalam mengamankan jaringan dari serangan berbasis volume seperti HTTP flood.

Gambar 12. Hasil Deteksi Ketiga Serangan
Sumber: Hasil Tangkapan Layar Penulis (2025)

Berdasarkan ketiga pengujian yang telah dilakukan suricata berhasil mendeteksi serta menghentikan tiga jenis serangan dari beberapa skenario pengujian. Log menunjukkan bahwa sistem mendeteksi serangan pertama berupa ICMP ping dari IP 192.168.1.10, yang dicatat sebagai "ICMP PING TERDETEKSI" dengan prioritas ancaman 3, menandakan aktivitas ping sweep atau network reconnaissance yang berpotensi digunakan untuk memetakan jaringan. Selanjutnya, sistem mendeteksi serangan kedua berupa port scanning dari IP 192.168.1.20, yang mencoba mengakses berbagai port tujuan secara bertahap. Serangan ini juga dikategorikan sebagai ancaman prioritas 3 dan diblokir otomatis oleh sistem, terbukti dari adanya status "[Drop]". Terakhir, serangan tipe denial of service (DoS) yang berasal dari IP 192.168.1.30 pada port 80. Serangan ini memiliki prioritas lebih tinggi, yaitu tingkat 2, karena bertujuan membanjiri layanan web dan menyebabkan gangguan operasional. Keseluruhan log ini menunjukkan bahwa suricata mampu secara efektif mengidentifikasi dan memblokir berbagai jenis serangan- mulai dari pengintaian sederhana hingga upaya penolakan layanan- secara rile-time, sehingga meningkatkan

perlindungan jaringan secara menyeluruh.

Tabel 3. *Log* Hasil *Suricata*

Waktu Deteksi	Jenis Serangan	IP Sumber→IP Tujuan	Tindakan Sistem
2025-07-10 21:23:06	ICMP *Ping*	192.168.1.10 → 192.168.1.1	*Dropped* (*Blocked*)
2025-07-10 10:30:20	*Port Scanning*	192.168.1.20 → 192.168.1.1	*Alert + Dropped*
2025-07-10 12:08:22	HTTP *Flood*	192.168.1.30 → 192.168.1.1	*Alert* (*Logged Only*)

Sumber: Hasil Rancangan Penulis (2025)

Berdasarkan log hasil deteksi suricata di Kantor Camat Lamasi Timur, sistem berhasil mengidentifikasi tiga jenis serangan, yaitu ICMP ping, port scanning, HTTP flood. Serangan ICMP ping dan port scanning berasal dari IP berbeda menuju IP target 192.168.1.1, dan langsung diblokir oleh sistem (dropped), menunujukkan konfigurasi ruleset yang responsif terhadap ancaman aktif. Sementara itu, serangan HTTP flood hanya dicatat (logged) tanpa pemblokiran, kemungkinan disebabkan oleh aturan yang belum mengatur tindakan drop untuk jenis serangan tersebut. Secara keseluruhan, IPS berbasis suricata mampu memberikan perlindungan yang cukup efektif terhadap lalu lintas berbahaya dalam jaringan kantor.

Evaluasi kinerja sistem dilakukan untuk menilai sejauh mana intrusion prevention system (IPS) berbasis suricata mampu memberikan perlindungan jaringan secara efektif tanpa mengganggu performa layanan jaringan di Kantor Camat Lamasi Timur. Evaluasi ini mencakup tiga aspek utama yaitu:

1. Efektivitas Deteksi dan Pencegahan

Suricata menunjukkan kemampuan tinggi dalam mendeteksi dan mencegah berbagai jenis serangan jaringan seperti ICMP ping, port scanning, dan HTTP flood. Hasil pengujian menunjukkan bahwa suricata secara akurat mengidentifikasi aktivitas mencurigakan berdasarkan rule yang telah ditentukan. Tingkat false positive (peringatan palsu) juga tergolong rendah, yang berarti sistem dapat membedakan antara trafik berbahaya dan trafik normal secara efektif. Ini menunjukkan bahwa kinerja deteksi suricata cukup andal dan responsif dalam menghadapi ancaman siber.

2. Stabilitas dan Kinerja Jaringan

Selama pengoperasian suricata, dilakukan pengukuran terhadap penggunaan CPU, memori, dan bandwidth jaringan. Hasilnya menunjukkan bahwa suricata hanya membutuhkan sumber daya sistem yang moderat, dengan peningkatan penggunaan CPU sekitar 5–10% dalam kondisi trafik normal hingga tinggi. Tidak ditemukan adanya gangguan atau penurunan kecepatan akses layanan jaringan internal, seperti aplikasi pelayanan masyarakat atau akses data lokal. Dengan demikian, suricata terbukti dapat berjalan secara efisien tanpa menimbulkan bottleneck atau gangguan performa jaringan.

3. Kemudahan Pengelolaan Sistem

Dari sisi manajemen, suricata relatif mudah diinstal dan dikonfigurasi oleh tim teknis yang memiliki kemampuan dasar administrasi jaringan. Log aktivitas yang dihasilkan disusun secara detail dan mudah dianalisis melalui file eve.json atau antarmuka visual jika dikombinasikan dengan dashboard seperti kibana atau EveBox. Admin juga dapat menyesuaikan aturan (ruleset) sesuai dengan pola ancaman lokal, sehingga sistem lebih fleksibel dan adaptif terhadap kebutuhan instansi.

4. Analisis Sistem

Analisis Keamanan dilakukan untuk menilai efektivitas penerapan sistem keamanan jaringan menggunakan intrusion prevention system berbasis suricata di Kantor Camat Lamasi Timur. Suricata sebagai alat keamanan open-source memberikan kemampuan deteksi dan pencegahan serangan, serta pemblokiran otomatis terhadap ancaman yang terdeteksi.

Hasil analisis menunjukkan bahwa suricata mampu:

- Mendeteksi berbagai jenis serangan seperti ICMP ping, port scanning, dan HTTP flood.
- Menghasilkan log serangan yang

mencatat timestamp, sumber dan tujuan IP, jenis protokol, serta tindakan (dropped/alert) yang diambil.

- Memblokir akses dari IP yang mencurigakan secara otomatis dengan berkoordinasi menggunakan IPTables, sehingga mencegah serangan mencapai sistem target.

Log suricata juga mencatat signature ID (SID) dari serangan yang berhasil dideteksi, menandakan bahwa aturan (rules) yang dikonfigurasi berjalan dengan baik. Dengan menggunakan rule signature log, sistem mampu mencocokkan pola serangan terhadap basis data signature yang telah diaktifkan.

Secara keseluruhan, sistem ini berhasil meningkatkan stabilitas jaringan, mengurangi resiko kebocoran data, serta mendukung keamanan layanan publik di Kantor Camat Lamasi Timur. Dengan adanya deteksi dan pencegahan otomatis, maka gangguan terhadap sistem pelayanan dapat diminimalisir, serta memungkinkan tim teknis untuk merespons insiden lebih cepat dan terukur.

Tabel 4. Hasil Analisis Sistem

Jenis Serangan	Waktu terdetksi	Respon Sistem	Keterangan
ICMP *Ping*	21:23:06	*Dropped* (*Blocked*)	Sistem mendeteksi serangan ICMP ±14 menit setelah dimulai dan memblokirnya.
Port Scanning	10:33:20	*Alert* + *Dropped*	Deteksi cepat (±3 menit), langsung direspons dengan pemblokiran oleh suricata.
HTTP *Flood*	12:08:22	*Alert* (*Logged*)	Sistem mencatat serangan tetapi tidak langsung memblokirnya.

Sumber: Hasil Rancangan Penulis (2025)

Berdasarkan tabel analisis sistem, menunjukkan kemampuan yang efektif dalam mendeteksi dan merespons berbagai jenis serangan. Suricata mampu mendeteksi serta memblokir serangan ICMP ping dan port scannimg secara otomatis, menunujukkan bahwa sistem telah dikonfigurasi dengan aturan (rule) yang sensitif terhadap ancaman umum. Khusus untuk serangan port scanning, sistem memberikan respons tercepat, yaitu dalam waktu sekitar 3 menit, menandakan tingkat kewaspadaan tinggi terhadap aktivitas pemindaian port yang biasanya digunakan untuk mencari celah keamanan. Sementara itu, pada serangan HTTP flood, suricata hanya mencatat aktivitas (logging) tanpa melakukan pemblokiran langsung, kemungkinan karena aturan yang digunakan belum menetapkan tindakan drop terhadap serangan tersebut. Secara keseluruhan, suricata terbukti responsif dan efektif, terutama terhadap serangan-serangan yang bersifat aktif dan berpotensi langsung mengganggu stabilitas jaringan.

Suricata mampu mendeteksi dan mencegah berbagai jenis serangan seperti ICMP ping, port scanning, HTTP flood, dan upaya akses tidak sah dengan akurasi tinggi dan tingkat false positive yang rendah. Selain itu, sistem ini tidak memberikan dampak negatif terhadap kinerja jaringan, karena penggunaan sumber daya sistem tetap stabil selama implementasi. Suricata juga mudah dikonfigurasi dan dikelola oleh admin jaringan lokal, serta tidak memerlukan biaya lisensi karena bersifat open-source, sehingga lebih efisien secara finansial. Dengan adanya logging dan monitoring yang terstruktur pihak pengelola jaringan dapat secara aktif memantau serta mengambil langkah mitigasi lebih cepat. Oleh karena itu, IPS berbasis suricata dinilai sangat layak dan efektif untuk diterapkan dalam lingkungan instansi pemerintahan seperti Kantor Camat.

Sebelum penerapan suricata, kondisi jaringan di Kantor Camat Lamasi Timur belum memiliki sistem perlindungan aktif terhadap serangan siber. Hal ini menyebabkan lalu lintas jaringan rentan terhadap berbagai ancaman seperti ICMP ping, port scanning, dan HTTP flood, dan potensi penyusupan malware yang tidak terdeteksi secara rile-time. Administraror jaringan hanya mengandalkan firewall dasar dan pengawasan manual yang tertabas. Akibatnya, sistem lebih lambat dalam merespons insiden keamanan, dan tidak jarang terjadi aktivitas mencurigakan yang luput dari perhatian. Namun, setelah suricata diaktifkan, jarang mengalami peningkatan signifikan dari sisi keamanan. Sistem mampu mendeteksi dan secara otomatis memblokir

lalu lintas mencurigakan berdasarkan rule yang telah dikonfigurasi. Selain itu, dashboard suricata memberikan visibilitas menyeluruh terhadap aktivitas jaringan, memungkinkan admin untuk mengambil tindakan cepat terhadap potensi ancaman. Performa jaringan pun tetap stabil, tanpa terjadi penurunan kecepatan akses atau ganguan layanan. Dengan adanya logging dan alert yang real-time , sistem menjadi lebih tanggap, aman, dan efisien dalam menghadapi ancaman siber yang berkembang.

Pembahasan Penelitian

Hasil dari metode penetration test secara keseluruhan untuk pengujian keamanan jaringan di Kantor Camat Lamasi Timur bisa dilihat melalui tabel 4 berikut ini. Pengujian ini mencakup berbagai jenis serangan untuk mengukur efektivitas instrusion prevention system (IPS) berbasis suricata dalam melaksanakan pendeteksian serta menghalau ancaman yang berpotensi membahayakan keamanan jaringan.

Tabel 5. Waktu Pengujian

Jenis Serangan	Awal Serangan	Waktu Terdeteksi	Terkirim
ICMP *Ping*	21:08:47	21:23:06	22:37:12
Port Scanning	10:30:20	10:33:08	10:35:10
HTTP Flood	12:00:10	12:08:22	12:10:11

Sumber: Hasil Rancangan Penulis (2025)

Pengujian dilakukan dengan tiga jenis serangan, yaitu serangan ICMP ping, port scanning, dan HTTP flood. Waktu mulai serangan dicatat, begitu pula waktu ketika instrusion prevention system (IPS) suricata berhasil mendeteksi dan menghalau serangan tersebut. Selain itu, waktu pengiriman peringatan kepada administrator juga dicatat untuk mengevaluasi kecepatan respons sistem dalam menghadapi ancaman keamanan jaringan. Hasil ini menunjukkan bahwa sistem IPS suricata mampu memberikan respon cepat dalam mendeteksi dan memblokir serangan yang masuk ke dalam jaringan Kantor Camat Lamasi Timur. Dengan demikian, sistem ini dinilai efektif dalam menjaga keamanan jaringan siber karena mampu memberikan deteksi dini terhadap ancaman, memungkinkan respons yang cepat, serta mendukung pengelolaan lalu lintas data yang aman dan terkendali. Selain itu, kombinasi antara konfigurasi perangkat keras dan perangkat lunak yang tepat juga berperan penting dalam mencegah akses tidak sah, serangan siber, serta kebocoran data. Sistem ini juga dapat dikembangkan dan disesuaikan dengan kebutuhan jaringan, baik dalam skala kecil maupun besar, sehingga menjadikannya solusi yang fleksibel dan andal dalam mendukung perlindungan infrastruktur TI secara menyeluruh.

Tabel 6. Hasil Pengujian

Jenis Serangan	Hasil Pengujian Sistem	Kesimpulan
ICMP *Ping*	Terdeteksi	Berhasil
Port Scanning	Terdeteksi	Berhasil
HTTP Flood	Terdeteksi	Berhasil

Sumber: Hasil Rancangan Penulis (2025)

Dari tabel di atas, bisa diketahui bahwa pelaksanaan uji memperoleh hasil yang sejalan dengan yang diinginkan. Sistem suricata sukses mendeteksi dan menghalau setiap jenis serangan yang dilakukan oleh attacker dengan tepat waktu. Pendeteksian serangan meliputi:

1. ICMP ping: dimulai pada pukul 21:08:47 dan berhasil dideteksi oleh sistem pada pukul 21:23:06, dengan waktu paket terakhir tercatat pada pukul 22:37:12. Ini menunjukkan bahwa suricata mampu mendeteksi aktivitas ping yang mencurigakan dan memberikan peringatan kepada sistem keamanan.
2. Port scanning dilakukan pada pukul 10:30:20 dan terdeteksi oleh suricata dalam waktu relatif cepat, yaitu pada pukul 10:33:08. Paket terakhir dikirim pada pukul 10:35:10, yang menandakan bahwa sistem berhasil merespon dan memutuskan upaya pemindahan port secara aktif.
3. HTTP flood dimulai pada pukul 12:00:10 dan terdeteksi pada pukul 12:08:22, dengan waktu paket terakhir tercatat pada 12:10:11. Serangan ini mensimulasikan lalu lintas HTTP yang

tinggi secara terus-menerus. Suricata mampu mengenali anomali lalu lintas dan memberikan respon sebelum layanan jaringan terganggu lebih lanjut.

Pendeteksian dan pencegahan serangan dilakukan sesuai dengan skenario yang telah dirancang, mulai dari perancangan sistem hingga serangan ICMP ping, port scanning, dan HTTP flood. Ancaman berhasil terdeteksi dan diblokir secara real-time, membuktikan bahwa IPS suricata mampu mengamankan jaringan secara efektif. Keberhasilan ini menunjukkan bahwa konfigurasi suricata dan aturan yang diterapkan sudah optimal dalam mendeteksi serta menghalau serangan, sehingga jaringan di Kantor Camat Lamasi Timur tetap terlindungi dari potensi ancaman siber.

Tabel 7. Hasil Implementasi

No	Aspek	Jenis Serangan	Hasil yang dicapai
1	Instalasi Suricata	-	*Suricata* berhasil diinstall dengan benar di server yang memantau lalu lintas jaringan kantor
2	Konfigurasi Mode IPS	*DDos*	*Suricata* berhasil mendeteksi serangan *Ddos* yang mencoba membanjiri *server* dengan lalu lintas berlebihan
3	SQL *Injection*	Serangan SQL *Injection*	Serangan SQL *Injection* melalui HTTP berhasil dideteksi oleh *suricata*
4	*Port Scanning*	Serangan *Port Scanning*	*Suricata* mampu mendeteksi upaya pemindaian port dari attacker dan memberikan peringatan dini terhadap potensi eksploitasi jaringan.
5	Kecepatan dan Kinerja Jaringan	-	Kinerja jaringan tidak terpengaruh signifikan oleh *suricata* meskipun berada dalam mode IPS, dengan penurunan minimal
6	Pemeliharaan dan Pembaruan	-	Pembaruan Berkala dilakukan pada rules *suricata* dan versi *suricata* untuk menjaga efektivitas deteksi ancaman

Sumber: Hasil Rancangan Penulis (2025)

Berdasarkan Tabel 5, implementasi sistem keamanan jaringan berbasis IPS dengan suricata di Kantor Camat Lamasi Timur menunjukkan kinerja yang efektif. Instalasi berhasil pada server pemantau lalu lintas, dan konfigurasi dalam mode IPS mampu mendeteksi serangan DDoS secara real-time, membuktikan respons sistem terhadap ancaman berjalan dengan baik.

Selain itu, suricata berhasil mendeteksi aktivitas port scanning dan serangan SQL Injection melalui protokol HTTP, menunjukkan kemampuannya dalam mengidentifikasi ancaman terhadap sistem dan basis data. Dari sisi performa, implementasinya tidak berdampak signifikan pada kecepatan jaringan, bahkan saat dijalankan dalam mode IPS, dengan penurunan kinerja yang sangat minimal.

Pemeliharaan dan pembaruan dilakukan secara berkala melalui update rules dan versi Suricata untuk menjaga efektivitas deteksi ancaman siber. Secara keseluruhan, implementasi Suricata terbukti memperkuat keamanan jaringan di lingkungan kantor pemerintahan.

Tabel 8. Perbandingan Kondisi Keamanan Jaringan Sebelum dan Sesudah Implementasi IPS Berbasis *Suricata*

Aspek Keamanan	Sebelum Implementasi IPS	Sesudah Implementasi IPS
Deteksi Ancaman	Deteksi dilakukan secara manual atau terbatas pada *firewall* dasar	Otomatis dan *real-time* melalui *signature* dan *anomaly-based detection*
Respon terhadap Serangan	Terlambat, bergantung pada laporan manual	Cepat, otomatis memblokir aktivitas mencurigakan
Logging dan Monitoring	Terbatas, *log* tidak terpusat	Terpusat dan lengkap melalui EVE JSON *log*
Lalu Lintas Mencurigakan	Sulit diidentifikasi	Dapat terindetifikasi dengan detail (IP, protokol, *playload*)
Pencegahan Serangan	Tidak ada mekanisme pencegahan langsung	Ada fitur *block*/drop untuk mencegah serangan aktif
Pemantauan *real-time*	Tidak tersedia	Tersedia melalui *dashboard* seperti *kibana*/ELK
Akurasi Deteksi	Rentan *false negative* (serangan tidak terdeteksi)	Lebih akurat, dapat dikustomisasi dengan *rule update*
Kepatuhan Keamanan	Tidak sesuai standar	Mendeteksi standar keamanan jaringan (ISO 27001, dsb)

Sumber: Hasil Rancangan Penulis (2025)

Sebelum penerapan IPS suricata, sistem keamanan jaringan di Kantor Camat Lamasi Timur bersifat pasif dan terbatas. Deteksi terhadap serangan jaringan masih mengandalkan firewall dasar atau pemantauan manual yang tidak mampu mengenali pola serangan kompleks. Hal ini menyebabkan banyak potensi ancaman tidak terdeteksi hingga berdampak pada sistem. Setelah implementasi suricata, kemampuan deteksi meningkat signifikan berkat fitur deep packet inspection dan rule-based detection, yang memungkinkan pengenalan berbagai serangan seperti Dos, ICMP ping, dan scanning port secara rile-time.

Dalam hal pencegahan, sebelumnya tidak terdapat sistem otomatis untuk memblokir serangan, sehingga respons terhadap insiden cenderung lambat dan

bersifat reaktif. Dengan suricata, sistem secara otomatis dapat mencegah serangan sebelum menimbulkan kerusakan, melalui konfigurasi rule yang memblokir trafik berbahaya. Monitoring aktivitas jaringan pun mengalami peningkatan signifikan. Jika sebelumnya visibilitas terhadap lalu lintas jaringan terbatas, kini dengan suricata seluruh aktivitas dapat dianalisis secara mendalam sehingga pola anomali atau percobaan intrusi dapat segera terdeteksi. Kemampuan monitoring jaringan meningkat signifikan dengan suricata, yang memungkinkan analisis mendalam terhadap lalu lintas, metadata, dan pola komunikasi antarhost. Administrator dapat cepat mendeteksi anomali, aktivitas mencurigakan, dan percobaan intrusi. Suricata juga mendukung integrasi dengan platform visualisasi untuk pemantauan data secara real-time. Secara keseluruhan, suricata meningkatkan efisiensi respons insiden serta pengawasan jaringan yang sebelumnya terbatas.

Pencatatan log dan pelaporan insiden sebelum implementasi juga minim dan tidak terstruktur, menyulitkan proses audit maupun investigasi. Setelah Suricata digunakan, log serangan terdokumentasi secara otomatis dan dapat diintegrasikan dengan sistem pelaporan visual seperti ELK stack, memudahkan analisis dan pelacakan insiden. Dari sisi respons terhadap insiden, suricata memberikan reaksi yang cepat dan otomatis terhadap berbagai ancaman, seperti memblokir IP sumber serangan secara langsung berdasarkan signature atau rule yang telah diterapkan. Mekanisme ini memungkinkan sistem untuk menangani potensi serangan tanpa campur tangan manusia secara langsung, sehingga mengurangi waktu respons secara signifikan. Hal ini sangat berbeda dengan sistem sebelumnya yang bergantung penuh pada deteksi manual dan kecepatan respons teknisi, yang berisiko menimbulkan keterlambatan dalam penanganan serangan. Dengan kemampuan otomatisasi ini, suricata meningkatkan efisiensi, akurasi, dan keandalan dalam perlindungan jaringan secara menyeluruh.

Skala perbandingan kondisi keamanan jaringan sebelum dan sesudah implementasi IPS berbasis suricata, disusun secara ringkas dengan skala penilaian 1–5, di mana:

- 1 = Sangat Rendah
- 2 = Rendah
- 3 = Cukup
- 4 = Tinggi
- 5 = Sangat Tinggi

Tabel 9. Skala Perbandingan Implementasi IPS *suricata*

Aspek Keamanan	Skor Sebelum	Skor Sesudah	Keterangan
Deteksi Serangan	2	5	Deteksi terbatas sebelumnya; *suricata* memberikan deteksi *real-time* dan akurat
Pencegahan Serangan	1	5	Tidak ada pencegahan otomatis sebelum; sekarang langsung memblokir serangan
Monitoring Lalu Lintas Jaringan	2	4	Dulu manual dan tidak lengkap; kini lebih detail dan sistematis
Pencatatan dan *log* Inseden	1	4	Sebelumnya sangat terbatas; kini *log* lengkap dan terintegrasi
Respons terhadap Ancaman	2	5	Respons lambat dulu; sekarang otomatis dan cepat
Visibilitas Jaringan	2	4	Sebelumnya minim; sekarang menyeluruh dengan dukungan *rule* dan *alerting*
Tingkat Keamanan Keseluruhan	2	5	Keamanan meningkat drastis setelah implementasi IPS *suricata*

Sumber: Hasil Rancangan Penulis (2025)

Setelah implementasi IPS berbasis suricata, terjadi peningkatan signifikan dalam berbagai aspek keamanan jaringan. Pada aspek deteksi serangan, sebelumnya sistem hanya mampu mengenali serangan dasar atau bahkan tidak mampu mendeteksi ancaman yang lebih kompleks. Namun setelah suricata diterapkan, kemampuan deteksi menjadi sangat tinggi karena sistem mampu menganalisis paket data secara mendalam dan mendeteksi berbagai jenis serangan secara real-time, dengan skor meningkat dari 2 menjadi 5. Pencatatan dan log insiden mengalami perubahan besar. Jika sebelumnya pencatatan log sangat minim atau tidak terdokumentasi dengan baik, kini setiap kejadian terekam secara rinci dan dapat diintegrasikan dengan sistem pelaporan seperti ELK stack. Hal ini meningkatkan skor dari 1 menjadi 4. Dalam hal respon terhadap ancaman, sebelumnya membutuhkan waktu

karena tergantung pada intervensi teknisi, namun setelah implementasi IPS, sistem merespons otomatis dalam hitungan detik, menjadikan skor naik dari 2 menjadi 5. Untuk visibilitas jaringan, sebelum implementasi hanya sedikit informasi yang bisa dianalisis dari lalu lintas data. Sekarang dengan adanya analisis rule-based dan alerting system, visibilitas meningkat signifikan, dari 2 menjadi 4. Keseluruhan, tingkat keamanan jaringan secara umum menunjukkan peningkatan paling signifikan, dari 2 menjadi 5, menandakan bahwa jaringan kini jauh lebih aman, terpantau, dan tahan terhadap ancaman siber.

Penerapan sistem ini membuktikan bahwa suricata, sebagai aplikasi open-source untuk intrusion prevention system (IPS), dapat digunakan secara efektif di instansi pemerintah dengan sumber daya terbatas. Suricata mampu menganalisis lalu lintas jaringan secara real-time, mendeteksi berbagai jenis serangan seperti ICMP ping, port scanning, dan HTTP flood, serta menghasilkan log yang rinci untuk keperluan audit dan analisis forensik. Selain itu, suricata mendukung berbagai protokol jaringan modern dan dapat diintegrasikan dengan sistem pemantauan seperti ELK stack untuk visualisasi data yang lebih informatif. Keberhasilan implementasi ini menunjukkan bahwa dengan perencanaan yang matang, konfigurasi yang tepat, dan pengelolaan yang berkelanjutan, solusi keamanan berbasis open-source seperti suricata dapat menjadi alternatif andal untuk memperkuat pertahanan jaringan di sektor pemerintahan.

4. KESIMPULAN

Berdasarkan hasil penelitian dan penerapan sistem keamanan jaringan menggunakan intrusion prevention system (IPS) berbasis suricata pada Kantor Camat Lamasi Timur, dapat disimpulkan bahwa suricata berhasil diimplementasikan sebagai sistem keamanan yang mampu mendeteksi dan mencegah berbagai ancaman siber seperti ICMP ping, port scanning, dan HTTP flood melalui pendekatan berbasis rules atau signature. Integrasi suricata dengan IPTables juga berfungsi dengan baik, terutama jika pengaturan dan penerapan aturannya dilakukan secara tepat, sehingga dapat meningkatkan performa serta kemampuan deteksi serangan pada jaringan. Sistem yang diusulkan terbukti mampu meningkatkan keamanan dan kestabilan jaringan, serta mengurangi risiko kebocoran data dan gangguan layanan, menggantikan sistem sebelumnya yang hanya mengandalkan firewall dan antivirus tanpa mekanisme deteksi dini. Penerapan sistem ini membuktikan bahwa Suricata sebagai solusi open-source dapat efektif digunakan di instansi pemerintah dengan sumber daya terbatas, asalkan didukung perencanaan dan pengelolaan yang baik.

5. DAFTAR PUSTAKA

Abdillah, Z., Adytia, P., & Fahmi, M. (2024). Implementasi Intrusion Detection System (IDS) Suricata Untuk Mendeteksi Serangan DDoS Menggunakan Metode TAARA Pada Jaringan Internet di Pixel Esport Arena Samarinda (Doctoral dissertation, STMIK atkerasjaringan. (Diakses, 29 juni 2021).

Adesty, I., Prabowo, W. A., & Sidiq, M. F. (2020). Penerapan Intrusion Prevention System (IPS) Suricata Sebagai Pengamanan Dari Serangan Distributed Denial of Service (DDoS).

Anam, M. K., Sudyana, D., Noviciatie, A., & Lizarti, N. (2020). Optimalisasi Penggunaan Virtualbox Sebagai Virtual Computer Laboratory Untuk Simulasi Jaringan Dan Praktikum Pada SMK Taruna Mandiri Pekanbaru J- PEMAS STMIK Amik Riau. Http://Jurnal.Sar.Ac.Id/Index.Php/J-PEMAS Optimal, Vol 1(2), 37–44.

Anggoro, B. S. (2019). Implementasi Intrusion Prevention System Berbasis Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Grahamedia Informasi (Doctoral dissertation, Program Studi Teknik Informatika FTI-UKSW).

Aulia, A. R., Alwi, E. I., & Gaffar, A. W. M. (2024). Perancangan Sistem Keamanan Jaringan Intrusion Prevention System Menggunakan Suricata Dan IPTables. LINIER: Literatur Informatika dan Komputer, 1(3), 235-240.

Duniait. 2020. Macam – Macam Perangkat Keras Jaringan Komputer Pengertian BesertaFungsinya.https://www.duniait.web. id/2020/07/macammacamperangk An-Nuur 13.2 (2023).

Haryono, Eko. "Metodologi Penelitian Kualitatif Di Perguruan Tinggi Keagamaan Islam." Widya Cipta Dharma).

Hermawan, A., T. Hartati dan Y. A. Wijaya. 2022. Analisa Keamanan Data Melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad. Jurnal Informatika: Jurnal Pengembangan IT. Vol. 7, No. 3, h. 125–130.

Hermawan, R. (2021). Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux. STRING (Satuan Tulisan Riset dan Inovasi Teknologi), 6(2), 210-216

Nurwijayanti, K. N. "Analisa Jaringan Lokal Area Network (Lan) Di Salah Satu Hotel Wilayah Jakarta Timur." Jurnal Ilmiah Matrik 23.3 (2021): 251-259.

Pramudana, K., Yasa, N., Ekawati, N., & Setiawan, P. (2023). Determinants of operational performance of pharmaceutical wholesalers' companies in Bali province. Uncertain Supply Chain Management, 11(3), 961-976.

Purnama, M. E. (2020). Implementasi Management Bandwidth dan Radius Server Pada SMK Telenika Palembang (Doctoral dissertation, STMIK Palcomtech).

Riska, R., & Alamsyah, H. (2021). Penerapan Sistem Keamanan Web Menggunakan Metode Web Aplication Firewall. JURNAL AMPLIFIER: JURNAL ILMIAH BIDANG TEKNIK ELEKTRO DAN KOMPUTER, 11(1), 37-42.

Rivaldi, O., & Marpaung, N. L. (2023). Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata. Jurnal Inovtek Polbeng Seri Informatika, 8(1), 141-153.

Serafica Gischa. (2023). Definisi Kajian Teori, Cara Membuat, dan Contohnya Halaman all – Kompas.com. Diakses pada 23 November 2023, dari KOMPAS.com website: https://www.kompas.com.

Setiawan, H., Gumilar, N., & Rahmawati, D. (2022). Media PembelajaranInovatif Game Based Learning Pointer pada Materi Topologi Jaringan Komputer. Jurnal FORTECH, 3(2), 57-63.

Suhendi, H., & Cahyo, W. D. (2021). Perancangan dan Implementasi Keamanan Jaringan Menggunakan Snort sebagai Intrusion Prevention System (IPS) pada Jaringan Internet STEI ITB. Naratif: Jurnal Nasional Riset, Aplikasi dan Teknik Informatika, 3(2), 60-68