# Implementasi Security Onion untuk Monitoring Serangan Port Scanning

Muhammad Ryan[1], Amri[2*], Muhammad Davi[3]

[1,2,3] *Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
*Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA*
[2]amri@pnl.ac.id

***Abstrak* – Keamanan jaringan merupakan aspek penting yang harus dijaga untuk memastikan ketersediaan layanan sekaligus melindungi data dari ancaman siber. Salah satu teknik serangan yang sering digunakan adalah port scanning, yaitu upaya penyerang untuk menemukan port terbuka yang dapat dimanfaatkan. Selain itu, serangan Distributed Denial of Service (DDoS) juga kerap digunakan untuk melemahkan atau melumpuhkan layanan dengan membanjiri jaringan menggunakan lalu lintas berlebih. Penelitian ini bertujuan menilai efektivitas Security Onion, sebuah sistem deteksi intrusi berbasis open source, dalam mendeteksi serangan terhadap MikroTik CHR yang terhubung langsung ke jaringan publik. Pengujian dilakukan dengan meluncurkan serangan dari jaringan luar menggunakan perangkat Kali Linux yang menargetkan alamat IP publik MikroTik. Topologi penelitian terdiri atas MikroTik CHR sebagai gateway, Security Onion sebagai sistem pemantauan melalui port mirroring, serta perangkat penyerang dari internet. Hasil pengujian menunjukkan bahwa Security Onion berhasil mendeteksi aktivitas port scanning dan DDoS secara konsisten, dengan tingkat deteksi mencapai 100% berdasarkan perhitungan Attack Detection Rate (ADR). Temuan ini membuktikan bahwa Security Onion mampu memberikan peringatan dini terhadap serangan dari jaringan luar serta berperan penting dalam meningkatkan keamanan jaringan berbasis MikroTik.**
**Kata kunci :** ***DdoS, Intrusion Detection System, MikroTik CHR, Port Scanning, Security Onion***

***Abstract – Network security is an essential aspect that must be maintained to ensure service availability and protect data from cyber threats. One of the most common attack techniques is port scanning, in which attackers attempt to find open ports that can be exploited. In addition, Distributed Denial of Service (DDoS) attacks are also frequently used to weaken or disable services by overwhelming the network with excessive traffic. This study aims to evaluate the effectiveness of Security Onion, an open-source intrusion detection system, in detecting attacks on MikroTik CHR devices directly connected to a public network. The experiment was conducted by launching attacks from an external network using a Kali Linux device targeting the public IP address of the MikroTik. The research topology consists of a MikroTik CHR as the gateway, Security Onion as the monitoring system through port mirroring, and an attacker device from the internet. The test results show that Security Onion successfully detected port scanning and DDoS activities consistently, achieving a 100% detection rate based on the Attack Detection Rate (ADR) calculation. These findings demonstrate that Security Onion is capable of providing early warnings against external network attacks and plays a crucial role in enhancing the security of MikroTik-based networks.***
***Keyword: DDoS, Intrusion Detection System, MikroTik CHR, Port Scanning, Security Onion.***

## I. PENDAHULUAN

### *A. Latar Belakang*

Keamanan jaringan semakin mendapat perhatian seiring maraknya kejahatan siber, seperti pencurian data, penipuan keuangan daring, peretasan situs, hingga penyebaran malware yang merusak sistem komputer [3]. Dalam dunia teknologi informasi, perangkat jaringan seperti MikroTik sering dipilih untuk membangun infrastruktur jaringan karena kemampuannya mengatur lalu lintas data sekaligus menyediakan fitur keamanan dengan biaya yang relatif terjangkau. Namun, meningkatnya ancaman serangan siber menimbulkan risiko serius, terutama terhadap serangan seperti port scanning dan Distributed Denial of Service (DDoS). Port scanning biasanya dilakukan penyerang untuk mengidentifikasi port yang terbuka pada suatu perangkat jaringan. Informasi tersebut dapat dimanfaatkan untuk mengeksploitasi celah keamanan dan memperoleh akses tidak sah [2]. Sementara itu, serangan DDoS berusaha melumpuhkan layanan dengan mengirimkan lalu lintas berlebihan. Tanpa sistem deteksi yang baik, serangan-serangan ini sulit diawasi secara real-time dan berpotensi menimbulkan kerugian yang lebih besar. Untuk menjawab tantangan tersebut, diperlukan sistem keamanan tambahan yang mampu memantau lalu lintas jaringan secara menyeluruh.

Salah satu platform yang banyak digunakan adalah Security Onion. Sistem ini merupakan distribusi Linux berbasis open source yang dirancang khusus untuk Network Security Monitoring (NSM). Di dalamnya terdapat berbagai komponen penting, seperti Suricata, Zeek, dan Kibana, yang memungkinkan administrator jaringan mendeteksi, menganalisis, sekaligus merespons ancaman siber secara lebih efektif. Security Onion dapat dijalankan sebagai sistem tunggal (standalone) maupun sebagai server yang mengelola data dari sensor lain [3]. Kebanyakan penelitian sebelumnya masih melakukan simulasi serangan dari jaringan lokal (local network), sehingga hasilnya belum sepenuhnya mencerminkan kondisi nyata. Pada penelitian ini, digunakan MikroTik CHR (Cloud Hosted Router) yang memiliki alamat IP publik dan berfungsi sebagai gateway utama antara

jaringan internal dan internet. Dengan demikian, serangan dilakukan dari jaringan luar menggunakan perangkat attacker berbasis Kali Linux. Cara ini lebih realistis karena menyerupai kondisi sebenarnya saat serangan berasal dari internet.

Seluruh lalu lintas yang masuk ke MikroTik digandakan melalui port mirroring dan dikirim ke Security Onion untuk dianalisis. Penelitian ini bertujuan mengimplementasikan Security Onion sebagai sistem deteksi ancaman pada MikroTik CHR yang terhubung ke internet. Dengan pendekatan ini, Security Onion diharapkan mampu mendeteksi berbagai serangan seperti port scanning dan DDoS yang berasal dari jaringan luar. Integrasi tersebut dapat meningkatkan keamanan jaringan berbasis MikroTik sekaligus memberikan gambaran nyata mengenai pentingnya penerapan Intrusion Detection System (IDS) dalam menjaga ketahanan infrastruktur jaringan modern.

*B. Dasar Teori*

1) *Keamanan Jaringan*: Sistem keamanan jaringan mengidentifikasi pengguna yang tidak memiliki akses ke jaringan untuk mencegah aktivitas yang tidak diinginkan. Dengan menghubungkan komputer satu sama lain melalui jaringan, baik kabel maupun nirkabel, orang lain dapat mengakses, mengubah, atau menghapus data dalam jaringan. Dengan menggunakan pendekatan berlapis, keamanan jaringan melindungi baik di dalam maupun di luar jaringan. Kerentanan ada di semua perangkat, jalur data, dan aplikasi. Setiap bisnis, dari perusahaan kecil hingga perusahaan terbesar, memerlukan keamanan jaringan untuk melindungi infrastruktur dan aset penting dari serangan yang berkembang pesat [4].

2) *Security Onion*: Security Onion adalah sebuah sistem yang dirancang untuk melakukan threat hunting, security monitoring dan log management. security onion juga menyatukan antara packet capture, intrusion detection, network meta data dan file analysis. Yang didalamnya terdapat beberapa services seperti Alerts, Hunt, PCAP, dan Cases, Playbook, osquery, Cyber Chef, Elastic search, Logstash, Kibana, Suricata, Zeek, and Wazuh. Dari penggabungan tersebut packet capture berfungsi untuk melakukan perekamanan segala aktifitas yang terjadi pada suatu lalu lintas jaringan [1].

3) *MikroTik:* MikroTik Router OS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk mengubah komputer menjadi router jaringan yang andal, termasuk berbagai fitur yang dibuat untuk jaringan IP dan jaringan nirkabel, cocok untuk digunakan oleh ISP dan penyedia hotspot [7].

4) *Port Scanning*: merupakan ancaman yang cukup serius bagi suatu sistem jaringan komputer, dan menjadi hal yang sangat menguntungkan bagi para attacker. Dengan port scanning, attacker mendapatkan informasi-informasi berharga yang dibutuhkan dalam melakukan serangan. Dengan kata lain, melakukan port scanning ialah untuk mengidentifikasi port port yang terbuka, dan mengenali OS (Operating System) target. Para profesional keamanan jaringan dapat melakukan pemindaian ini untuk memastikan keamanan jaringan dan menemukan potensi kerentanan dengan menggunakan alat seperti Nmap [5].

5) *Brute Force*: Serangan brute force menggunakan trial and error untuk menebak info login, kunci enkripsi, atau menemukan halaman web yang tersembunyi. Peretas bekerja melalui semua kemungkinan kombinasi dengan harapan dapat menebak dengan benar. Serangan ini dilakukan dengan brute force yang berarti mereka menggunakan upaya paksa yang berlebihan untuk mencoba dan memaksa masuk ke akun pribadi [8].

6) *Distributed Denial of Service:* Serangan DDoS dilakukan dengan mengirimkan banyak paket ke dalam jaringan, menyebabkan perangkat jaringan tidak dapat berfungsi dengan baik. Serangan DDoS juga membutuhkan metode untuk mendeteksi kejadian pada server secara real time agar dapat dianalisa dan digunakan sebagai dasar sebagai bukti, yaitu dengan menggunakan Intrusion Detection System (IDS) pada server. DDoS telah terbukti menimbulkan ancaman terus menerus bagi pengguna Internet, perusahaan, dan infrastruktur. Sebaliknya, serangan jaringan merupakan bahaya [6].

## II. METODOLOGI PENELITIAN

*A. Metode dan Variabel Penelitian*

Pada penelitian ini menggunakan beberapa metode dalam penyusunan skripsi yaitu:

1) *Studi Literatur:* Menganalisa berbagai jenis bahan pustaka yang dapat dijadikan acuan penelitian ini seperti jurnal ilmiah, buku, tesis, artikel dan blog yang relevan dengan topik yang dibahas pada judul ini yang bertujuan untuk mendapatkan pemahaman yang lebih mendalam terhadap permasalahan utama dari penelitian yang sedang dilakukan.
2) *Perancangan Sistem:* Pada tahap ini penulis akan melakukan perancangan sistem keamanan jaringan mikrotik dengan menggunakan beberapa perangkat hardware seperti server, client, access point, switch dan mikrotik.
3) *Implementasi:* Setelah melakukan perancangan sistem dan memastikan jaringan yang dirancang telah selesai, tahap selanjutnya yaitu mengimplementasikan security onion berdasarkan desain yang telah dibuat, untuk mencegah serangan port scanning DDoS dan brute force.
4) *Pengujian dan Kesimpulan:* Setelah implementasi selesai maka akan dilakukan pengujian pada sistem keamanan jaringan mikrotik dan hasil pengujian apakah desain sistem yang dirancang sesuai dengan tujuan yang ingin dicapai peneliti serta membuat kesimpulan untuk

dapat menjadi rekomendasi pengembangan di masa depan.

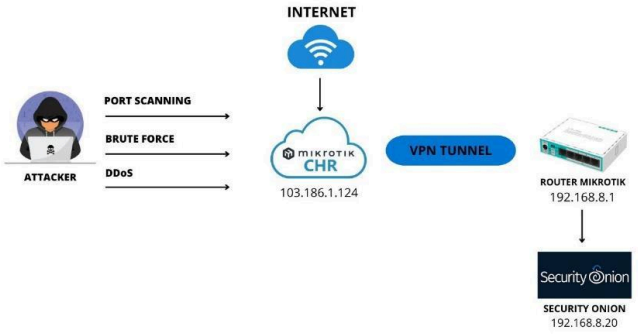
### B. *Data dan Pengumpulan Data*

Data primer dan sekunder digunakan dalam penelitian ini. Data primer diperoleh melalui observasi langsung di lokasi penelitian, sedangkan data sekunder diperoleh dengan membaca dan mempelajari literatur terkait, seperti jurnal, buku, dan penelitian sebelumnya. Semua sumber referensi dipilih berdasarkan relevansinya dengan penelitian ini. Beberapa metode pengumpulan data telah disebutkan diantaranya:

- Studi Pustaka Pengumpulan data dilakukan dengan membaca dan mempelajari literatur yang relevan dengan topik penelitian. Sumber-sumber ini dapat termasuk buku, artikel, jurnal, dan sumber lainnya.
- Observasi Proses di mana penulis melihat langsung objek yang akan diteliti untuk mengetahui keadaan sebenarnya. Pengamatan awal menggunakan metode ini.

### C. *Perancangan Sistem (Hardware/Software)*

Rancangan sistem yang dibuat bertujuan untuk merepresentasikan skenario nyata, yaitu ketika serangan berasal dari jaringan luar melalui internet. Pada penelitian ini digunakan MikroTik CHR yang telah memiliki alamat IP publik sebagai gateway utama, sehingga dapat diakses langsung dari jaringan eksternal. Lalu lintas yang masuk dan keluar dari MikroTik CHR kemudian disalin melalui mekanisme port mirroring untuk dipantau oleh Security Onion. memiliki perancangan sistem pada gambar 1 berikut.




Gambar 1. Rancangan Sistem

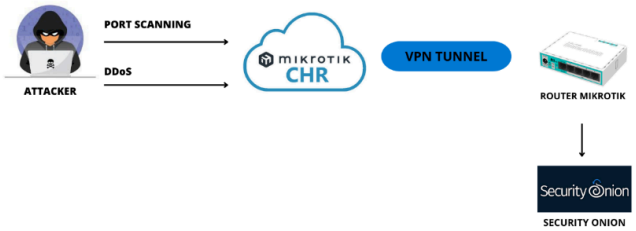
Berdasarkan gambar 1 terdapat 3 perangkat utama dan 1 layanan yang digunakan untuk membangun rancangan sistem.

1) *Layanan internet* berfungsi sebagai jalur komunikasi yang menghubungkan penyerang eksternal (attacker) dengan MikroTik CHR. Dengan adanya IP publik pada MikroTik CHR, perangkat tersebut dapat diakses langsung dari luar jaringan internal melalui koneksi internet.
2) *MikroTik CHR* merupakan perangkat yang berperan sebagai pengatur lalu lintas jaringan dengan fungsi utama sebagai gateway antara jaringan lokal dengan internet. Perangkat ini dilengkapi alamat IP publik, sehingga menjadi target utama serangan dari luar jaringan. Lalu lintas yang melewati MikroTik CHR kemudian diteruskan ke jaringan lokal melalui VPN tunnel. Selain itu, perangkat ini juga dikonfigurasi untuk melakukan port mirroring sehingga setiap serangan dapat dipantau dan dianalisis oleh Security Onion.
3) *Router MikroTik* lokal dengan alamat IP 192.168.8.1 berfungsi sebagai penghubung antara MikroTik CHR dan perangkat monitoring. Router ini menjadi titik distribusi lalu lintas jaringan internal sekaligus sumber data yang dikirimkan melalui port mirroring menuju Security Onion.
4) *Security Onion* merupakan sistem Network Security Monitoring (NSM) yang digunakan untuk mendeteksi dan menganalisis lalu lintas jaringan yang mencurigakan. Dengan dukungan komponen IDS/IPS seperti Suricata dan Zeek, Security Onion dapat memantau aktivitas serangan secara real time serta mencatat log untuk kebutuhan analisis lebih lanjut. Dalam penelitian ini, Security Onion berperan sebagai pusat deteksi terhadap seluruh serangan yang ditujukan ke MikroTik CHR.
5) *Attacker* merupakan perangkat simulasi yang digunakan untuk melancarkan berbagai jenis serangan dari jaringan eksternal melalui internet. Dalam penelitian ini, serangan yang diuji meliputi port scanning untuk mendeteksi port terbuka dan DDoS untuk membanjiri lalu lintas jaringan. Serangan-serangan ini bertujuan untuk menguji sejauh mana efektivitas Security Onion dalam mendeteksi ancaman dari luar jaringan.

### D. *Teknik Pengujian*

Teknik pengujian dalam penelitian ini dirancang untuk memastikan efektivitas integrasi antara Security Onion dan MikroTik CHR dalam mendeteksi serangan jaringan dari luar. Tahap awal dilakukan dengan menguji fungsi sistem guna memastikan alur komunikasi berjalan baik, khususnya dalam mendeteksi aktivitas port scanning. Selanjutnya, dilakukan simulasi serangan dari attacker eksternal yang diarahkan ke alamat IP publik MikroTik CHR. Serangan pertama berupa port scanning menggunakan Nmap untuk menguji kemampuan Security Onion dalam mendeteksi pemindaian port secara real time. Setelah itu, dilakukan pengujian serangan Distributed Denial of Service (DDoS) menggunakan Hping3 maupun LOIC (Low Orbit Ion Cannon) untuk menilai kemampuan sistem dalam mencatat serta menganalisis lalu lintas berlebihan akibat serangan dari luar jaringan. Pengujian berikutnya adalah serangan brute force ke layanan autentikasi, seperti SSH, dengan memanfaatkan Hydra untuk mencoba berbagai kombinasi kata sandi secara berulang. Uji coba ini bertujuan memastikan Security Onion dapat mendeteksi aktivitas percobaan login yang mencurigakan serta mencatatnya sebagai upaya intrusi yang berisiko. Serangan yang berasal dari mesin penyerang diarahkan ke gateway

MikroTik CHR. Seluruh lalu lintas yang melewati MikroTik kemudian digandakan melalui mekanisme port mirroring dan dikirimkan ke Security Onion. Traffic yang diterima oleh Security Onion dianalisis menggunakan komponen Suricata dan Zeek untuk mendeteksi pola serangan, seperti port scanning dan DDoS. Hasil analisis selanjutnya dicatat dan divisualisasikan melalui Kibana, sehingga administrator dapat memantau secara real-time aktivitas berbahaya yang terjadi di dalam jaringan. Dengan adanya alur ini, efektivitas sistem dalam mendeteksi serta mendokumentasikan serangan dapat dievaluasi secara lebih komprehensif, sebagaimana ditunjukkan pada gambar 2 ilustrasi alur deteksi serangan dengan security onion.




Gambar 2. Ilustrasi Alur Deteksi Serangan dengan Security Onion

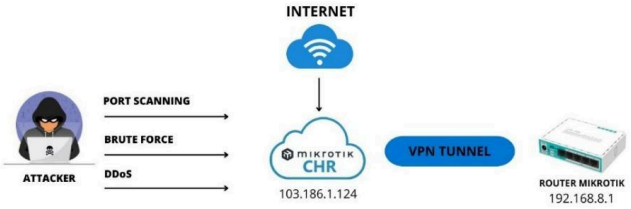
Pada ilustrasi tersebut dapat dilihat bahwa Security Onion berperan sebagai sistem deteksi intrusi yang memproses salinan lalu lintas dari MikroTik CHR. Setiap paket yang masuk ke jaringan diperiksa menggunakan Suricata dan Zeek untuk mengidentifikasi pola serangan. Hasil analisis kemudian disimpan dan divisualisasikan melalui Kibana sehingga administrator dapat dengan mudah memantau aktivitas berbahaya secara real-time. Dengan adanya alur ini, proses pengujian menjadi lebih sistematis karena serangan yang dilakukan dapat terdeteksi, tercatat, dan dievaluasi secara komprehensif. Efektivitas sistem dievaluasi dari jumlah dan jenis alert yang dihasilkan Suricata dan Zeek. Analisis dilakukan dengan menilai keakuratan log, konsistensi alert, serta kecepatan respons sistem terhadap serangan. Sebagai pembanding, pengujian juga dilakukan pada jaringan tanpa Security Onion. Hasilnya diharapkan memberi gambaran peran Security Onion dalam meningkatkan keamanan jaringan berbasis MikroTik CHR, khususnya terhadap serangan port scanning dan DDoS.

## III. HASIL DAN PEMBAHASAN

### *A. Hasil Penelitian*

Penelitian ini bertujuan untuk mengimplementasikan Security Onion sebagai sistem pemantauan keamanan jaringan (Network Security Monitoring) pada infrastruktur berbasis MikroTik CHR dengan IP publik. Fokus penelitian adalah mendeteksi ancaman siber yang berasal dari jaringan luar, meliputi serangan port scanning, brute force, dan DDoS. Lingkungan pengujian dibangun dengan memanfaatkan VirtualBox untuk menjalankan Security Onion serta server internal, sementara MikroTik CHR berfungsi sebagai gateway dengan IP publik yang menjadi target serangan. Penyerang (attacker) menggunakan Kali Linux yang terkoneksi melalui internet, sehingga skenario lebih mendekati kondisi nyata dibandingkan hanya uji pada jaringan lokal. Hasil pengujian menunjukkan bahwa Security Onion berhasil mendeteksi seluruh serangan yang disimulasikan. Deteksi dilakukan melalui komponen seperti Suricata dan Zeek, dengan data hasil uji disajikan dalam bentuk log serta visualisasi pada Kibana. Sistem mampu mencatat informasi penting, antara lain alamat IP penyerang, jenis serangan, serta waktu kejadian. Berdasarkan hasil tersebut, dapat disimpulkan bahwa Security Onion mampu meningkatkan deteksi dan respons terhadap ancaman siber pada MikroTik CHR, khususnya dalam skenario serangan dari jaringan luar.

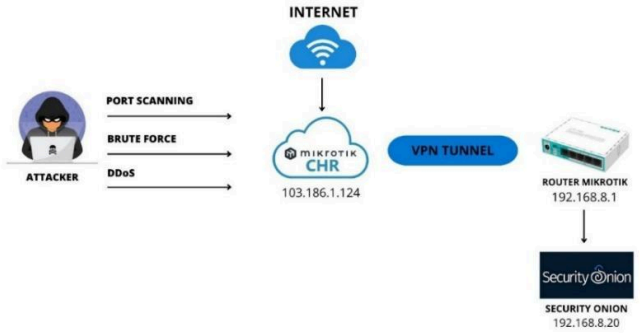
Sebelum dilakukan implementasi Security Onion, jaringan penelitian hanya mengandalkan MikroTik CHR sebagai gateway utama dengan alamat IP publik. Dalam kondisi ini, MikroTik berfungsi untuk mengatur lalu lintas data dan melakukan port forwarding, tetapi tidak memiliki kemampuan khusus untuk melakukan deteksi atau analisis terhadap aktivitas serangan. Ketika serangan dari luar jaringan diarahkan ke MikroTik, misalnya serangan port scanning dan Distributed Denial of Service (DDoS), perangkat hanya meneruskan lalu lintas tanpa memberikan peringatan. Administrator jaringan tidak dapat mengetahui secara detail alamat IP penyerang, jenis serangan yang dilakukan, maupun waktu terjadinya aktivitas tersebut. Satu-satunya indikasi yang mungkin terlihat hanyalah adanya penurunan kinerja jaringan atau gangguan layanan pada perangkat target. Kondisi ini menunjukkan keterbatasan keamanan jika hanya mengandalkan perangkat gateway. Tanpa adanya sistem pendeteksi intrusi, serangan dapat berlangsung tanpa diketahui sehingga meningkatkan risiko gangguan maupun eksploitasi lebih lanjut. Oleh karena itu, diperlukan penerapan Intrusion Detection System (IDS) berupa Security Onion untuk melengkapi fungsi keamanan jaringan agar aktivitas berbahaya dapat dipantau dan dianalisis secara real-time. Topologi sebelum implementasi security onion dapat dilihat pada gambar 3 berikut.




Gambar 3. Topologi Jaringan Sebelum Implementasi Security Onion

Pada topologi sebelum implementasi, jaringan hanya menggunakan MikroTik CHR sebagai gateway utama yang terhubung ke internet. Seluruh lalu lintas dari luar, termasuk serangan port scanning dan DDoS, langsung diarahkan menuju MikroTik tanpa adanya pemantauan dari sistem IDS. Kondisi ini menyebabkan aktivitas berbahaya tidak dapat terdeteksi secara detail, karena MikroTik hanya berfungsi sebagai pengatur lalu lintas data tanpa fitur analisis keamanan.

Setelah dilakukan implementasi Security Onion, topologi jaringan penelitian mengalami perubahan dengan penambahan sistem IDS sebagai komponen pemantauan. Security Onion dihubungkan melalui mekanisme port mirroring pada MikroTik sehingga seluruh lalu lintas jaringan yang melewati gateway juga disalin menuju sistem IDS untuk dianalisis. Pada kondisi ini, serangan dari luar jaringan seperti port scanning dan DDoS tidak hanya diteruskan ke target, tetapi juga dapat dideteksi oleh Security Onion. Setiap paket yang masuk diperiksa oleh komponen Suricata dan Zeek untuk menemukan pola serangan, kemudian hasil deteksinya dicatat dan divisualisasikan melalui Kibana. Dengan cara ini, administrator jaringan dapat mengetahui detail aktivitas berbahaya, termasuk alamat IP penyerang, jenis serangan yang dilakukan, port yang diserang, serta waktu kejadian. Perbedaan signifikan dibandingkan kondisi sebelumnya adalah kini jaringan memiliki lapisan keamanan tambahan yang mampu memberikan deteksi dini. Jika pada kondisi awal serangan tidak dapat dipantau, setelah implementasi Security Onion administrator dapat memantau aktivitas mencurigakan secara real-time dan mengambil langkah mitigasi yang lebih cepat dan tepat. Setelah Security Onion berhasil diimplementasikan, jaringan penelitian kini memiliki sistem deteksi intrusi (IDS) yang terintegrasi. Security Onion dihubungkan dengan MikroTik melalui mekanisme port mirroring sehingga setiap lalu lintas yang melewati gateway juga dikirimkan salinannya untuk dianalisis. Dengan adanya tambahan ini, aktivitas serangan yang sebelumnya tidak terpantau kini dapat dideteksi secara real-time, sebagaimana ditunjukkan pada gambar 4 berikut.




Gambar 4. Topologi Jaringan Sesudah Implementasi Security Onion

Pada topologi tersebut terlihat bahwa Security Onion telah menjadi komponen tambahan di dalam jaringan. Setiap serangan dari luar, baik port scanning dan DDoS, tidak hanya diteruskan ke target, tetapi juga digandakan menuju Security Onion. Sistem IDS kemudian memproses paket tersebut menggunakan komponen Suricata dan Zeek untuk mendeteksi pola serangan. Hasil analisisnya dicatat dan divisualisasikan melalui Kibana sehingga administrator dapat melihat informasi detail, seperti alamat IP penyerang, port yang diserang, jenis serangan, serta waktu kejadian. Dengan kondisi ini, perbedaan yang paling menonjol dibandingkan sebelum implementasi adalah jaringan tidak lagi buta terhadap aktivitas berbahaya. Administrator kini memiliki kemampuan untuk memantau, menganalisis, dan menindaklanjuti serangan dengan lebih cepat serta akurat, sehingga sistem keamanan jaringan menjadi lebih kuat.

*B. Pembahasan Penelitian*

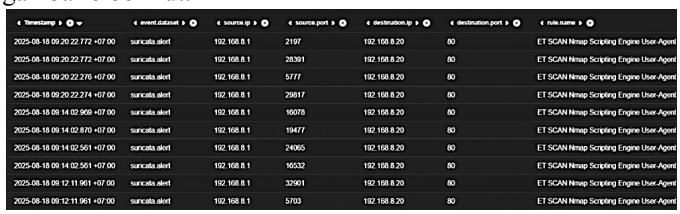
Pada penelitian ini, Security onion digunakan sebagai sistem deteksi intrusi (IDS) untuk memantau lalu lintas jaringan dan mendeteksi adanya aktivitas yang mencurigakan. Sistem ini dibangun menggunakan sejumlah komponen open source seperti Suricata, Zeek, dan Kibana yang bekerja secara terintegrasi untuk merekam dan menganalisis data dari setiap koneksi jaringan yang terjadi. Melalui antarmuka visual yang disediakan, penulis dapat memantau hasil deteksi secara real time serta mengakses informasi detail yang berkaitan dengan potensi serangan, seperti alamat IP sumber, IP tujuan, jenis protokol yang digunakan, dan waktu kejadian. Selama proses pengujian, Security onion menunjukkan kemampuannya dalam menangkap aktivitas yang tidak wajar di jaringan, termasuk serangan yang disimulasikan oleh penulis. Setiap aktivitas yang dianggap sebagai ancaman akan tercatat dalam bentuk log dan alert, yang kemudian dapat digunakan sebagai bahan analisis untuk memahami pola serangan yang terjadi. Dengan kemampuan ini, Security onion berperan penting sebagai sistem peringatan dini yang membantu administrator jaringan dalam mengambil langkah cepat untuk mencegah kerusakan atau gangguan lebih lanjut. Keandalan sistem ini memperkuat pentingnya penerapan IDS dalam membangun lingkungan jaringan yang aman dan tangguh terhadap berbagai ancaman siber.

Pengujian ini dilakukan untuk memastikan bahwa Security Onion mampu mengenali dan mencatat aktivitas mencurigakan yang berpotensi membahayakan jaringan. Salah satu metode yang digunakan dalam simulasi ini adalah pemindaian port (port scanning), yaitu teknik dasar yang umum dipakai penyerang untuk mengidentifikasi layanan yang terbuka pada suatu sistem sebelum melanjutkan ke tahap eksploitasi. Untuk keperluan ini digunakan tool bernama Nmap pada mesin penyerang, dengan menargetkan alamat IP publik milik MikroTik CHR. Pemindaian dilakukan terhadap IP publik 103.186.1.124, yang berfungsi sebagai pintu masuk jaringan penelitian ini. Pengujian ini bertujuan untuk mengetahui apakah sistem deteksi intrusi pada Security Onion dapat merekam aktivitas pemindaian port dari jaringan luar.

Perintah yang dijalankan adalah nmap -sV 103.186.1.124 untuk mengidentifikasi port yang terbuka beserta layanan yang berjalan pada router MikroTik CHR. Hasil pemindaian menunjukkan adanya beberapa port terbuka, antara lain port 21 (FTP), 22 (SSH), 23 (Telnet), 80 (HTTP), 2000 (Bandwidth-test), dan 8291 (Winbox service). Temuan ini mengindikasikan bahwa MikroTik CHR menyediakan sejumlah layanan yang berpotensi menjadi celah keamanan jika tidak diamankan dengan baik. Seluruh aktivitas pemindaian tersebut berhasil dicatat oleh Security Onion, yang kemudian ditampilkan dalam bentuk log untuk dianalisis lebih lanjut. Hasil pemindaian ditunjukkan pada gambar 5 berikut.

Gambar 5. Hasil Pemindaian Port pada IP Publik MikroTik CHR

Berdasarkan hasil pemindaian pada gambar 5 menunjukkan bahwa serangan diarahkan ke alamat IP publik MikroTik CHR (103.186.1.124). Akan tetapi, karena telah dilakukan konfigurasi port forwarding, port yang terdeteksi merupakan layanan milik MikroTik lokal. Dari hasil scanning teridentifikasi beberapa port terbuka, yaitu port 22 (SSH), port 23 (Telnet), port 2000 (Bandwidth-test), dan port 8291 (Winbox service). Kondisi ini memperlihatkan bahwa layanan internal tetap terekspos ke jaringan luar sehingga dapat diakses oleh penyerang apabila tidak diamankan dengan baik. Informasi yang diperoleh dari hasil pemindaian ini kemudian menjadi dasar bagi analisis lebih lanjut terkait potensi kerentanan jaringan. Setelah proses pemindaian port dilakukan dari mesin Kali Linux menggunakan tool Nmap terhadap alamat IP publik MikroTik CHR, sistem Security Onion yang telah dikonfigurasi sebelumnya memberikan respons terhadap aktivitas tersebut. Berdasarkan deteksi yang dilakukan oleh Suricata dengan menggunakan rule set dari Emerging Threats (ET), aktivitas pemindaian berhasil dicatat dan diklasifikasikan sebagai potensi serangan. Log yang dihasilkan menunjukkan bahwa Security Onion mampu mengenali pola karakteristik dari Nmap Scripting Engine, yang umumnya dipakai penyerang untuk melakukan eksplorasi lebih lanjut terhadap layanan-layanan yang terbuka. Deteksi ini menjadi bukti bahwa sistem IDS berfungsi dengan baik dalam mengenali aktivitas mencurigakan yang berasal dari jaringan luar. Seluruh data hasil serangan terekam secara otomatis dan dapat ditinjau kembali melalui dashboard analitik seperti Kibana. Dengan demikian, sistem mampu memberikan gambaran menyeluruh terkait adanya upaya serangan port scanning yang ditujukan ke alamat IP publik MikroTik CHR. Hasil deteksi tersebut ditampilkan pada gambar 6 berikut.



| Timestamp | event.dataset | source.ip | source.port | destination.ip | destination.port | rule.name |
|---|---|---|---|---|---|---|
| 2025-08-18 09:20:22.772 +07:00 | suricata.alert | 192.168.8.1 | 2197 | 192.168.8.20 | 80 | ET SCAN Nmap Scripting Engine User-Agent |
| 2025-08-18 09:20:22.772 +07:00 | suricata.alert | 192.168.8.1 | 28391 | 192.168.8.20 | 80 | ET SCAN Nmap Scripting Engine User-Agent |
| 2025-08-18 09:20:22.276 +07:00 | suricata.alert | 192.168.8.1 | 5777 | 192.168.8.20 | 80 | ET SCAN Nmap Scripting Engine User-Agent |
| 2025-08-18 09:20:22.274 +07:00 | suricata.alert | 192.168.8.1 | 29817 | 192.168.8.20 | 80 | ET SCAN Nmap Scripting Engine User-Agent |
| 2025-08-18 09:14:02.909 +07:00 | suricata.alert | 192.168.8.1 | 16078 | 192.168.8.20 | 80 | ET SCAN Nmap Scripting Engine User-Agent |
| 2025-08-18 09:14:02.870 +07:00 | suricata.alert | 192.168.8.1 | 19477 | 192.168.8.20 | 80 | ET SCAN Nmap Scripting Engine User-Agent |
| 2025-08-18 09:14:02.561 +07:00 | suricata.alert | 192.168.8.1 | 24065 | 192.168.8.20 | 80 | ET SCAN Nmap Scripting Engine User-Agent |
| 2025-08-18 09:14:02.561 +07:00 | suricata.alert | 192.168.8.1 | 16532 | 192.168.8.20 | 80 | ET SCAN Nmap Scripting Engine User-Agent |
| 2025-08-18 09:12:11.961 +07:00 | suricata.alert | 192.168.8.1 | 32901 | 192.168.8.20 | 80 | ET SCAN Nmap Scripting Engine User-Agent |
| 2025-08-18 09:12:11.961 +07:00 | suricata.alert | 192.168.8.1 | 5703 | 192.168.8.20 | 80 | ET SCAN Nmap Scripting Engine User-Agent |

Gambar 6. Log Deteksi Pemindaian Nmap oleh Suricata

Hasil log pada gambar 6 memperlihatkan bahwa Security Onion berhasil mendeteksi aktivitas port scanning yang dilakukan melalui serangan Nmap terhadap alamat IP publik MikroTik CHR. Deteksi ini tercatat sebagai alert ET SCAN Nmap Scripting Engine User-Agent Detected yang dihasilkan oleh Suricata. Informasi pada log menunjukkan detail penting seperti alamat IP sumber, port yang digunakan, alamat tujuan, serta waktu terjadinya aktivitas. Hal ini menegaskan bahwa sistem mampu mengenali pola serangan dari jaringan luar dan mencatatnya secara real time, sehingga dapat dijadikan acuan dalam proses analisis lebih lanjut terhadap potensi ancaman. Berdasarkan hasil uji coba, serangan port scanning yang diarahkan dari mesin Kali Linux menuju alamat publik MikroTik CHR (103.186.1.124) berhasil terdeteksi oleh Security Onion. Namun, pada log yang terekam terlihat bahwa sumber serangan tercatat berasal dari alamat 192.168.8.1. Perbedaan ini disebabkan oleh mekanisme Network Address Translation (NAT) dan port forwarding yang diterapkan pada MikroTik CHR, di mana lalu lintas dari internet diteruskan ke jaringan internal sebelum dipantau oleh Security Onion. Dengan demikian, meskipun alamat IP yang muncul pada log berbeda dari IP penyerang yang sebenarnya, sistem tetap mampu menangkap pola serangan secara utuh dan mengklasifikasikannya sebagai aktivitas berbahaya. Hal ini menunjukkan bahwa implementasi sistem deteksi masih berjalan efektif dalam mengenali ancaman meskipun terdapat perbedaan representasi alamat IP akibat konfigurasi NAT. Deteksi serangan terjadi secara instan sesaat setelah perintah pemindaian dijalankan. Entri log langsung tercatat pada Security Onion dan dapat ditinjau melalui dashboard analitik seperti Kibana. Respons cepat ini membuktikan bahwa sistem IDS beroperasi secara aktif dan responsif terhadap upaya serangan. Dalam praktik nyata, pemindaian port semacam ini sering digunakan penyerang sebagai tahap awal untuk menemukan celah layanan sebelum melancarkan eksploitasi lanjutan. Oleh karena itu, keberhasilan Security Onion dalam mendeteksi pola serangan ini tidak hanya menunjukkan efektivitas sistem, tetapi juga menegaskan bahwa konfigurasi serta rule set yang diterapkan telah berjalan sesuai dengan fungsinya dalam menjaga keamanan jaringan. Keberadaan komponen seperti Suricata sebagai mesin deteksi, rule set dari Emerging Threats, serta integrasi dengan Kibana dan Elasticsearch, memungkinkan pemantauan dilakukan secara real time dan memudahkan respons cepat terhadap potensi ancaman. Untuk menilai sejauh mana Security Onion konsisten dalam mendeteksi aktivitas port scanning, dilakukan pengujian berulang sebanyak dua puluh kali dengan target alamat IP publik MikroTik CHR (103.186.1.124). Pengujian ini bertujuan melihat konsistensi sistem dalam mencatat setiap aktivitas pemindaian meskipun dijalankan dalam waktu dan pola yang berbeda. Seluruh hasil dicatat, baik percobaan yang berhasil menghasilkan alert maupun yang tidak terdeteksi pada dashboard Security Onion. Dengan pendekatan ini, diperoleh gambaran yang lebih objektif mengenai performa sistem, sekaligus memungkinkan perhitungan persentase keberhasilan deteksi menggunakan metode Attack Detection

Rate (ADR). Rekapitulasi hasil pengujian ditunjukkan pada tabel 1 berikut.

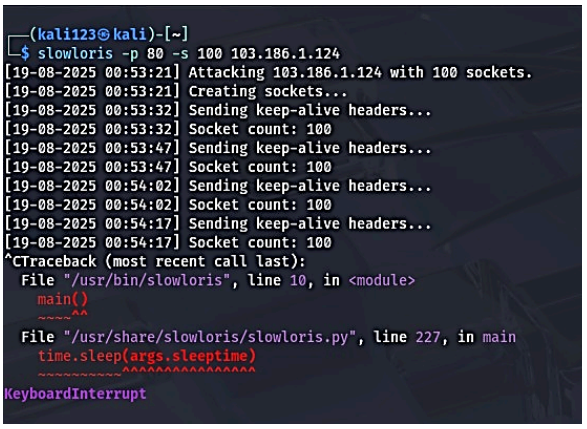
TABEL I
HASIL PENGUJIAN DAN DETEKSI PORT SCANNING OLEH SECURITY ONION DENGAN JENIS SERANGAN ET SCAN N,MAP

| No | Tanggal/Waktu | › Penyerang | P Target | Status Deteksi |
|---|---|---|---|---|
| 1 | )25-08-17 /03:41 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 2 | )25-08-17 /04:13 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 3 | )25-08-17 /02:41 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 4 | )25-08-17 /20:11 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 5 | )25-08-18 /09:12 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 6 | )25-08-18 /09:14 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 7 | )25-08-18 /09:20 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 8 | )25-08-18 /20:44 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 9 | )25-08-18 /20:49 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 10 | )25-08-25 /10:12 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 11 | )25-08-25 /10:18 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 12 | )25-08-25 /10:25 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 13 | )25-08-25 /10:33 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 14 | )25-08-26 /09:05 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 15 | )25-08-26 /09:12 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 16 | )25-08-26 /09:20 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 17 | )25-08-26 /09:27 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 18 | )25-08-26 /09:34 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 19 | )25-08-26 /09:41 | 92.168.8.1 | 2.168.8.20 | Deteksi |
| 20 | )25-08-26 /09:50 | 92.168.8.1 | 2.168.8.20 | Deteksi |

Berdasarkan data pada tabel 1, dari dua puluh kali percobaan serangan port scanning yang diarahkan ke alamat IP publik MikroTik CHR (103.186.1.124), seluruh aktivitas berhasil terdeteksi oleh Security Onion. Hasil ini membuktikan bahwa sistem mampu mengenali pola lalu lintas mencurigakan secara konsisten pada setiap percobaan. Dengan menggunakan rumus Attack Detection Rate (ADR), diperoleh tingkat efektivitas deteksi sebesar ADR= (Jumlah Serangan Terdeteksi)/(Jumlah Total Serangan) 100% =20/20 100%=100% Nilai ADR sebesar 100% menunjukkan bahwa *Security Onion* berhasil mendeteksi seluruh aktivitas pemindaian jaringan yang dilakukan selama pengujian. Capaian ini menegaskan bahwa sistem bekerja secara optimal dalam mengidentifikasi dan mencatat aktivitas *port scanning*, sekaligus memperlihatkan keandalannya sebagai sistem deteksi dini yang dapat membantu administrator jaringan dalam memberikan respons cepat terhadap potensi ancaman.

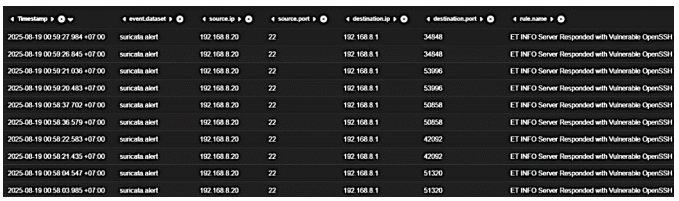
### *C. Simulasi Serangan Lanjutan (DDoS)*

BSetelah melakukan pengujian serangan port scanning, penelitian dilanjutkan dengan simulasi serangan Distributed Denial of Service (DDoS). Pada tahap ini digunakan perangkat uji Slowloris yang dijalankan dari mesin Kali Linux sebagai sumber serangan. Serangan Slowloris dipilih karena metode ini menargetkan lapisan aplikasi (application layer) dengan cara membanjiri server melalui banyak koneksi HTTP yang tidak pernah diselesaikan. Setiap koneksi dipertahankan tetap aktif dengan mengirimkan permintaan secara parsial (incomplete request), sehingga server korban kehabisan sumber daya untuk melayani permintaan sah dari pengguna lain. Pada skenario ini, serangan diarahkan ke alamat IP publik MikroTik CHR yang telah dikonfigurasi sebagai target. Perintah Slowloris dijalankan dari terminal Kali Linux dengan parameter tertentu untuk membuka ratusan koneksi secara bersamaan. Tampilan perintah saat eksekusi serangan dapat dilihat pada gambar 7 berikut.




Gambar 7. Serangan DDoS Slowloris dari Kali Linux ke MikroTik CHR

Gambar 7 memperlihatkan proses serangan DDoS Slowloris yang dieksekusi dari terminal Kali Linux. Pada tampilan tersebut terlihat bahwa perintah berhasil membuka sejumlah soket menuju port 80 (HTTP) pada alamat IP publik MikroTik CHR. Setiap soket kemudian dijaga agar tetap aktif dengan cara mengirimkan keep-alive headers, sehingga koneksi tidak pernah diselesaikan. Hal ini menyebabkan server target dipaksa mempertahankan ratusan koneksi palsu secara bersamaan, yang pada akhirnya akan menguras sumber daya sistem. Kondisi ini menandakan bahwa serangan telah berjalan sebagaimana mestinya dari sisi penyerang. Dengan strategi yang digunakan Slowloris, layanan HTTP pada target berpotensi mengalami penurunan kinerja, seperti melambatnya respons hingga kegagalan menerima permintaan baru dari pengguna sah. Simulasi ini juga menggambarkan bagaimana serangan application layer dapat terlihat sederhana, tetapi berdampak signifikan terhadap ketersediaan layanan jaringan. Peluncuran serangan dari mesin Kali Linux menjadi bukti awal bahwa sistem target benar-benar menerima trafik berlebih dalam bentuk koneksi HTTP tidak normal. Tahap selanjutnya adalah memantau sistem deteksi intrusi pada Security Onion untuk memastikan apakah aktivitas anomali yang dihasilkan dari serangan Slowloris dapat dikenali dan tercatat secara real time dalam bentuk log maupun alert. Setelah serangan dijalankan dari sisi penyerang, tahap berikutnya adalah melakukan verifikasi pada sistem deteksi untuk memastikan apakah aktivitas anomali tersebut berhasil dikenali. Pemantauan dilakukan melalui Security Onion yang telah dikonfigurasi untuk menerima salinan trafik dari MikroTik CHR. Hasil pengamatan menunjukkan bahwa komponen deteksi, yaitu Suricata, berhasil mencatat adanya aktivitas mencurigakan yang dihasilkan oleh serangan Slowloris. Deteksi ini muncul dalam bentuk alert yang menandakan adanya pola koneksi tidak normal menuju layanan HTTP target. Log hasil deteksi tersebut dapat dilihat pada gambar 8 berikut.



| Timestamp | event.dataset | source.ip | source.port | destination.ip | destination.port | rule.name |
|---|---|---|---|---|---|---|
| 2025-08-19 00:59:27.984 +07:00 | suricata.alert | 192.168.8.20 | 22 | 192.168.8.1 | 34648 | ET INFO Server Responded with Vulnerable OpenSSH |
| 2025-08-19 00:59:26.845 +07:00 | suricata.alert | 192.168.8.20 | 22 | 192.168.8.1 | 34648 | ET INFO Server Responded with Vulnerable OpenSSH |
| 2025-08-19 00:59:21.036 +07:00 | suricata.alert | 192.168.8.20 | 22 | 192.168.8.1 | 53996 | ET INFO Server Responded with Vulnerable OpenSSH |
| 2025-08-19 00:59:20.483 +07:00 | suricata.alert | 192.168.8.20 | 22 | 192.168.8.1 | 53996 | ET INFO Server Responded with Vulnerable OpenSSH |
| 2025-08-19 00:58:37.702 +07:00 | suricata.alert | 192.168.8.20 | 22 | 192.168.8.1 | 50858 | ET INFO Server Responded with Vulnerable OpenSSH |
| 2025-08-19 00:58:36.579 +07:00 | suricata.alert | 192.168.8.20 | 22 | 192.168.8.1 | 50858 | ET INFO Server Responded with Vulnerable OpenSSH |
| 2025-08-19 00:58:22.583 +07:00 | suricata.alert | 192.168.8.20 | 22 | 192.168.8.1 | 42092 | ET INFO Server Responded with Vulnerable OpenSSH |
| 2025-08-19 00:58:21.435 +07:00 | suricata.alert | 192.168.8.20 | 22 | 192.168.8.1 | 42092 | ET INFO Server Responded with Vulnerable OpenSSH |
| 2025-08-19 00:58:04.547 +07:00 | suricata.alert | 192.168.8.20 | 22 | 192.168.8.1 | 51320 | ET INFO Server Responded with Vulnerable OpenSSH |
| 2025-08-19 00:58:03.985 +07:00 | suricata.alert | 192.168.8.20 | 22 | 192.168.8.1 | 51320 | ET INFO Server Responded with Vulnerable OpenSSH |

Gambar 8. Log Deteksi Serangan DDoS Slowloris oleh Suricata pada Security Onion

Gambar 8 menampilkan hasil log deteksi yang ditangkap oleh Suricata pada Security Onion setelah serangan Slowloris dijalankan. Dari tampilan tersebut dapat dilihat bahwa sistem berhasil mengenali adanya aktivitas jaringan yang tidak wajar dengan mengklasifikasikannya sebagai alert. Informasi detail pada log mencakup alamat IP sumber serangan yang berasal dari mesin penyerang, alamat IP tujuan yang merupakan target serangan, serta protokol komunikasi yang digunakan. Selain itu, tercatat pula waktu terjadinya serangan yang memungkinkan administrator jaringan untuk mengetahui secara tepat kapan aktivitas anomali tersebut berlangsung. Deteksi ini membuktikan bahwa Security Onion tidak hanya mampu menangkap serangan sederhana seperti port scanning, tetapi juga efektif dalam menghadapi serangan yang lebih kompleks pada lapisan aplikasi (application layer). Hal ini terlihat dari bagaimana sistem dapat mengenali pola koneksi HTTP yang mencurigakan akibat banyaknya permintaan parsial yang dikirimkan oleh Slowloris. Tanpa adanya IDS seperti Security Onion, lalu lintas berbahaya semacam ini akan sulit teridentifikasi karena serangan tidak memanfaatkan volume data besar, melainkan teknik manipulasi koneksi yang lebih halus. Lebih lanjut, keberhasilan Security Onion dalam mendeteksi serangan ini menunjukkan peran pentingnya sebagai sistem peringatan dini (early warning system). Informasi yang terekam pada log dapat dijadikan bahan analisis mendalam bagi administrator untuk menelusuri pola serangan, melakukan mitigasi, dan memperkuat kebijakan keamanan jaringan. Dengan demikian, integrasi Security Onion bersama MikroTik CHR terbukti mampu memberikan lapisan perlindungan tambahan dalam menghadapi ancaman siber, khususnya serangan DDoS berbasis application layer seperti Slowloris. Untuk memastikan konsistensi deteksi, serangan DDoS dengan Slowloris tidak hanya dilakukan sekali, melainkan diulang sebanyak dua puluh kali percobaan. Pengulangan ini bertujuan untuk melihat apakah sistem IDS Security Onion mampu mengenali seluruh serangan yang diarahkan ke IP publik MikroTik CHR secara berulang. Setiap percobaan dijalankan dengan parameter yang sama, yaitu menargetkan port 80 pada alamat IP publik MikroTik CHR, menggunakan 100 soket aktif yang dipertahankan dengan pengiriman keep-alive headers. Dari sisi penyerang, serangan berjalan stabil dan terus membanjiri layanan HTTP pada target. Sementara dari sisi sistem deteksi, Security Onion diharapkan mencatat aktivitas tersebut sebagai anomali dan menghasilkan alert melalui Suricata. Rekapitulasi hasil pengujian ditunjukkan pada tabel 2 berikut.

TABEL II.
HASIL PENGUJIAN DAN DETEKSI DDOS OLEH SECURITY ONION JENIS SERANGAN DDOS SLOWLORIS

| No | Tanggal/Waktu | IP Penyerang | IP Target | Status Deteksi |
|---|---|---|---|---|
| 1 | 2025-08-18 /01:15 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 2 | 2025-08-18 /01:25 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 3 | 2025-08-18 /01:35 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 4 | 2025-08-18 /01:45 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 5 | 2025-08-18 /01:55 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 6 | 2025-08-18 /02:05 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 7 | 2025-08-18 /02:15 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 8 | 2025-08-18 /02:25 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 9 | 2025-08-18 /02:35 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 10 | 2025-08-18 /02:45 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 11 | 2025-08-25 /09:10 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 12 | 2025-08-25 /09:20 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 13 | 2025-08-25 /09:30 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 14 | 2025-08-25 /09:40 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 15 | 2025-08-25 /09:50 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 16 | 2025-08-26 /08:15 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 17 | 2025-08-26 /08:25 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 18 | 2025-08-26 /08:35 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 19 | 2025-08-26 /08:45 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |
| 20 | 2025-08-26 /08:55 | 192.168.8.1 | 192.168.8.20 | Terdeteksi |

Berdasarkan tabel 2, terlihat bahwa seluruh percobaan serangan DDoS menggunakan Slowloris berhasil dideteksi oleh Security Onion. Dari dua puluh kali percobaan yang dilakukan, semuanya menghasilkan alert yang tercatat pada dashboard Suricata. Hal ini menunjukkan bahwa sistem IDS mampu memberikan deteksi yang konsisten meskipun serangan dilakukan berulang dengan parameter yang sama. Dengan demikian, tingkat keberhasilan deteksi dapat dihitung menggunakan rumus Attack Detection Rate (ADR) sebagai berikut: ADR= (Jumlah Serangan Terdeteksi)/(Jumlah Total Serangan) 100% =20/20 100%=100%

Nilai ADR sebesar 100% menunjukkan bahwa Security Onion berhasil mendeteksi seluruh aktivitas serangan DDoS menggunakan Slowloris yang dilakukan selama pengujian. Capaian ini menegaskan bahwa sistem bekerja secara optimal dalam mengidentifikasi dan mencatat aktivitas anomali pada lapisan aplikasi (application layer), sekaligus memperlihatkan keandalannya sebagai sistem deteksi dini yang dapat membantu administrator jaringan dalam memberikan respons cepat terhadap potensi serangan DDoS. Selain itu, hasil ini juga membuktikan bahwa metode serangan Slowloris, meskipun memanfaatkan teknik koneksi parsial yang lebih halus dibandingkan serangan berbasis volume, tetap dapat terdeteksi secara konsisten oleh Security Onion. Dengan demikian, sistem ini tidak hanya efektif dalam menangani serangan sederhana, tetapi juga handal dalam menghadapi ancaman yang lebih kompleks yang menyasar stabilitas layanan jaringan.

## IV. KESIMPULAN

Berdasarkan hasil dan pembahasan pada penelitian yang telah dilakukan, dapat disimpulkan bahwa Security onion terbukti efektif dalam mendeteksi serangan port scanning dan DDoS pada jaringan MikroTik. Hal ini dibuktikan melalui pengujian simulasi yang menunjukkan sistem mampu mengenali dan mencatat aktivitas serangan secara real-time

menggunakan komponen seperti Suricata dan Zeek, serta menyajikan hasil pemantauan melalui antarmuka Kibana. Tingkat efektivitas sistem dalam mendeteksi serangan mencapai kategori sangat efektif berdasarkan perhitungan ADR (Attack Detection Rate). Jumlah serangan yang berhasil dideteksi oleh security onion sebanyak 20 dari 20 percobaan serangan port scanning yang dilakukan selama pengujian. Selain itu DDoS yang di simulasikan, menunjukkan bahwa security onion memiliki kemampuan deteksi yang konsisten dan akurat terhadap berbagai jenis serangan jaringan.

## REFERENSI


[1] A. Mukherjee, M. Ammar, and P. Vigneshwaran, "Implementation of Intrusion Detection System (IDS) Using Security Onion," in Lecture Notes in Networks and Systems, vol. 300, no. 10, pp. 685–704, 2022. https://link.springer.com/chapter/10.1007/978-3-030-84760-9_58

[2] D. K. Nurilahi, R. Munadi, S. Syahrial, and A. Bahri, "Penerapan Metode Naïve Bayes pada Honeypot Dionaea dalam Mendeteksi Serangan Port Scanning," ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika, vol. 10, no. 2, p. 309, 2022. https://ejurnal.itenas.ac.id/index.php/elkomika/article/view/5343

[3] F. Yohaness, "Analisa dan Perancangan Keamanan Jaringan Lokal Menggunakan Security Onion dan Mikrotik," Journal of Information System and Technology, vol. 1, no. 2, pp. 37–61, 2020. [Online]. Available: https://journal.uib.ac.id/index.php/joint/article/view/4309

[4] H. Alamsyah, R. -, and A. Al Akbar, "Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System," JOINTECS (Journal of Information Technology and Computer Science), vol. 5, no. 1, p. 17, 2020. https://doi.org/10.31328/jointecs.v5i1.1240

[5] I. M. Razzanda and M. Koprawi, "Implementasi IDS dan IPS terhadap Serangan TCP Port Scanning dan ICMP Flooding," The Indonesian Journal of Computer Science, vol. 13, no. 4, 2024. https://doi.org/10.33022/ijcs.v13i4.4212

[6] M. Syani, "Implementasi Intrusion Detection System (IDS) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Server (VPS)," The Development of Information Technology, vol. 1, no. 1, pp. 13–20, 2020. https://www.politeknikmeta.ac.id/meta/ojs/index.php/inkofar/article/view/155

[7] Y. Mulyanto and A. A. Fari, "Analisis Keamanan Login Router Mikrotik Dari Serangan Bruteforce Menggunakan Metode Penetration Testing (Studi Kasus: SMK Negeri 2 Sumbawa)," Jurnal Informatika, Teknologi dan Sains, vol. 4, no. 3, pp. 145–155, 2022. https://doi.org/10.51401/jinteks.v4i3.1897

[8] Y. Mulyanto, H. Herfandi, and R. C. Kirana, "Analisis Keamanan Wireless Local Area Network (WLAN) Terhadap Serangan Brute Force Dengan Metode Penetration Testing (Studi Kasus: RS H. Lmanambai Abdulkadir)," Jurnal Informatika Teknologi dan Sains (Jinteks), vol. 4, no. 1, pp. 26–35, 2022. https://doi.org/10.51401/jinteks.v4i1.1528