Deteksi Serangan Ddos Pada Jaringan Rt/Rw-Net Desa Ketanen Dengan Metode Intrusion Detection System (IDS) Menggunakan Snort

Zulhelmi Dwi Alfaeni[1], Nuniek Fahriani[2].
Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Surabaya
Jl. Raya Sutorejo No.59, Dukuh Sutorejo, Kec. Mulyorejo, Surabaya, Jawa Timur 60113
e-mail: [1]zulhelmidwialfaeni@gmail.com, [2]nuniekfahriani@ft.um-surabaya.ac.id.

Abstrak

RT/RW net adalah jaringan swadaya masyarakat yang mencakup wilayah RT/RW dengan menggunakan media kabel atau Wireless 2.4 GHz dan Hotspot sebagai alat komunikasi rakyat. Karena banyaknya client dan minimnya pengawasan pada jaringan ini. maka diperlukan sebuah sistem untuk menjaga keamanan jaringan tersebut yaitu Intrusion Detection System(IDS) yang digunakan untuk mendeteksi aktifitas yang mencurigakan dalam sebuah sistem atau jaringan dan melakukan analisis serta mencari bukti dari percobaan penyusupan. Pada penelitian ini, subuah IP address client atau koban dilakukan penyerangan dengan menggunakan DDOS attack, sehingga untuk mengetahui atau mendeteksi adanya serangan tersebut dapat dideteksi oleh snort. Berdasarkan hasil penelitian ini, dapat ditarik kesimpulan bahwa penerapan aplikasi SNORT dapat mendeteksi serangan-serangan jaringan melalui icmp, nmap, dan ddos. Metode intrusion Detection System adalah metode yang bisa mengoptimalkan tingkat keamanan jaringan komputer melalui pendeteksian serangan sehingga administrator jaringan dapat melakukan Tindakan pencegahan lebih awal.
***Kata Kunci**: RT/RW-net, DDoS, IDS, Snort.*

Abstract

RT/RW Net is a community-driven network that spans the RT/RW area using both cable and 2.4 GHz wireless media, and utilizes Hotspots as a means of communication for the public. Due to the large client base and minimal supervision on this network, a security system is necessary to maintain network security. This system is known as an Intrusion Detection System (IDS), which is employed to identify suspicious activities within a system or network. It conducts analysis and searches for evidence of intrusion attempts. In this research, a DDOS attack was executed against the IP address of a client or victim. To identify or detect the presence of such an attack, Snort was used. Based on the research findings, it can be concluded that the implementation of the SNORT application is capable of detecting network attacks, including ICMP, NMAP, and DDOS attacks. The Intrusion Detection System method is an approach that can enhance the security of a computer network by identifying attacks, enabling network administrators to take proactive measures.

***Keywords**: RT/RW-net, DDoS, IDS, Sort.*

1. PENDAHULUAN

Kemajuan yang signifikan dalam teknologi informasi telah memfasilitasi pertukaran informasi yang semakin cepat dan lebih kompleks. Berdasarkan survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pengguna internet di Indonesia mencapai 215,63 juta orang pada periode 2022-2023, mengalami peningkatan sebesar 2,67% dibandingkan dengan periode sebelumnya yang berjumlah 210,03 juta pengguna. [1]

Pengelolaan jaringan yang efisien akan memaksimalkan pemanfaatan informasi tersebut. Oleh karena itu, perlu pengaturan dan pemantauan yang cermat terhadap jaringan komputer agar pengiriman informasi berjalan lancar. Jaringan komputer dapat mengalami penurunan kinerja atau tidak optimal ketika disusupi oleh pihak lain demi keuntungan mereka. Menurut laporan yang dipublikasikan di situs web resmi Kementerian Komunikasi

dan Informatika, terdapat 90 juta serangan siber yang tercatat terjadi di Indonesia dari Januari hingga akhir Juni 2016. Serangan tersebut mencakup pencurian data, pemalsuan data, dan modifikasi data, seperti mengubah tampilan halaman situs web.[2]. Website menjembatani para penggunanya untuk mendapatkan berbagai macam informasi dari mana saja. alhasil kebutuhan akan informasi semakin meningkat.

RT/RW-Net adalah jaringan komputer swadaya masyarakat yang mencakup wilayah RT/RW dengan menggunakan media kabel atau Wireless 2.4 GHz dan Hotspot sebagai alat komunikasi rakyat. Jaringan ini tidak terikat oleh undang-undang atau birokrasi pemerintah. Pemanfaatan RT/RW Net ini bisa dijadikan sebagai sarana komunikasi online yang efektif bagi warga untuk berbagi informasi, berdiskusi, melakukan polling, atau bahkan mengadakan pemilihan ketua RT/RW, tanpa adanya batasan waktu dan jarak melalui email, chatting, dan portal web. Selain itu, fungsi utama RT/RW Net adalah menyediakan akses internet[3].

Salah satu cara untuk mengamankan sebuah informasi yaitu dengan memasang teknologi firewall. Firewall akan melakukan sebuah kebijakan keamanan dengan memberikan aturan-aturan dijaringan tersebut untuk akses keluar masuknya paket data pada jaringan. Namun, keamanan yang dilakukan firewall biasanya dirancang hanya untuk memblokir trafik-trafik yang mencurigakan tanpa tahu mana trafik-trafik yang berbahaya dan mana trafik yang tidak berbahaya. Sehingga paket firewall yang rasa itu berbahaya akan ditindaki oleh firewall.Oleh karena itu, dibutuhkan suatu sistem dalam menangani penyerangan disebuah jaringan atau ancaman-ancaman dari penyusup yang akan terjadi yaitu dengan menggunakan Teknik Intrusion Detection System (IDS)[4] Sistem Deteksi Intrusi (IDS) merupakan suatu teknik yang dapat diterapkan guna menemukan tindakan yang mencurigakan dalam sistem atau jaringan. IDS dapat memeriksa lalu lintas masuk dan keluar dalam sistem atau jaringan, melakukan evaluasi, dan mencari jejak upaya peretasan (intrusi).[5].

2. METODE PENELITIAN

Penelitian ini menggunakan metode Intrusion Detection Syestem (IDS) yang digunakan untuk mendeteksi aktifitas yang mencurigakan dalam sebuah sistem atau jaringan dan melakukan analisis serta mencari bukti dari percobaan penyusupan. Pada penelitian ini, subuah IP address client atau koban dilakukan penyerangan dengan menggunakan Kali Linux, sehingga untuk mengetahui atau mendeteksi adanya serangan tersebut dapat dideteksi oleh snort. Yang dimana pengujian ini bertujuan untuk mengetahui keamanan jaringan[6].

2.1. Jenis Data

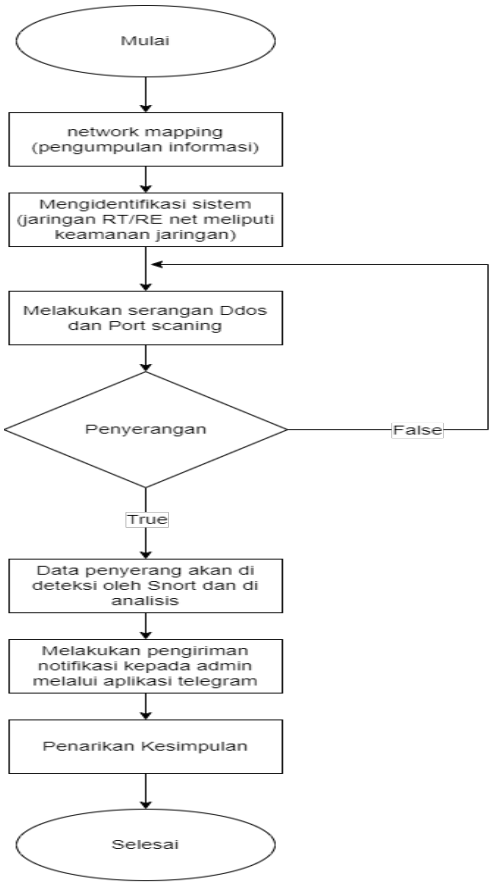
Jenis data yang digunakan dalam penelitian ini adalah:

1. Data primer yaitu data yang di peroleh dan dipati langsung dari jaringan RT/RW net Di desa ketanen
2. Data sekunder yaitu data yang diperoleh dari buku. Jurnal ilmiah dan internet.

2.2. Metode Pengumpulan Data

1. Observasi : melakukan pengamatan terhadap jaringan local RT/RW net di desa ketanen.
2. Wawancara : pengumpulan informasi dari tanya jawab terhadap salah satu pegawai dan pengelola RT/RW net Umumnya penelitian kualitatif menggunakan jumlah sampel kecil. Bahkan pada kasus tertentu menggunakan hanya 1 informan saja. Setidaknya ada dua syarat yang harus dipenuhi dalam menentukan jumlah informan yaitu kecukupan dan kesesuaian [7]
3. Studi Pustaka Tahap penting dalam proses penelitian adalah melakukan studi kepustakaan setelah peneliti menentukan topik penelitian. Pada langkah ini,

peneliti melakukan penelusuran literatur yang relevan dengan teori yang terkait dengan topik penelitian [8] Studi pustaka melibatkan pencarian referensi jurnal secara online dan kunjungan ke perpustakaan untuk mencari buku-buku yang relevan dengan topik penelitian.



Gambar 1. Tahapan Penelitian

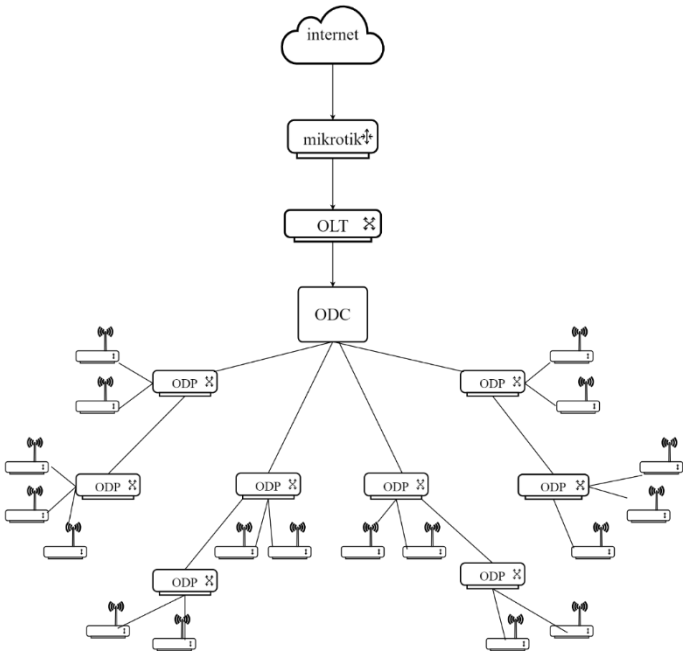
2.3. Metode Pengolahan Data

Pengolahan awal data dalam penelitian deteksi serangan yang terjadi pada jaringan RT/RW net dengan metode Intrusion Detection System menggunakan snort adalah sebagai berikut:

1. Mengidentifikasi sistem keamanan jaringan RT/RW net melalui observasi dan wawancara kepada administrator.
2. Melakukan instalasi snort sebagai Intrusion Detection System.
3. Melakukan pengujian serangan menggunakan Ddos
4. Menerapkan snort pada jaringan RT/RW net.

2.4. Topologi Jaringan RT/RW net desa ketanen

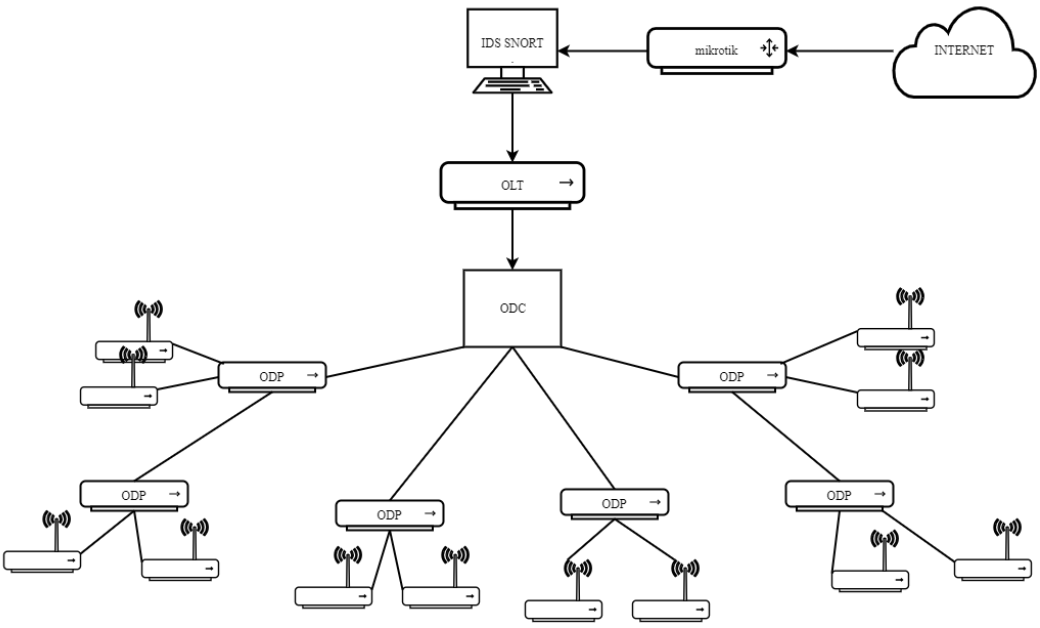
Topologi merupakan hal mendasar dalam membentuk sebuah jaringan, topologi jaringan pada RT/RW net di desa ketanen menggunakan topologi tree gabungan dari topologi star dengan topologi bus. Topologi jaringan ini juga dikenal sebagai topologi jaringan hierarkis. Biasanya, topologi ini digunakan untuk menghubungkan berbagai tingkat pusat dengan hirarki yang berbeda. Tingkat yang lebih rendah digambarkan pada lokasi fisik yang lebih bawah, sementara tingkat yang lebih tinggi terletak di atasnya. Jenis topologi jaringan ini sangat sesuai untuk sistem jaringan komputer[9].



Gambar 2. Topologi Jaringan RT/RW net desa ketanen

2.5. Usulan Perancangan Sistem

Perancangan sistem untuk mengatasi permasalahan pada jaringan RT/RW net di desa ketanen meliputi pengawasan terhadap keamanan jaringan melalui tools/software yang berguna untuk pencegahan terhadap serangan jaringan yang mungkin saja bisa dilakukan pada saat yang tidak terduga. Software bisa meliputi snort yang bertujuan untuk mendeteksi adanya serangan jaringan dan menangkap paket – paket data. Pengujian serangan pada jaringan local RT/RW net desa ketanen yang telah menggunakan metode IDS snort menggunakan Ddos dan port scaning. Berikut ini merupakan alur pengujian jaringan yang telah menggunakan snort.



Gambar 3. Usulan Perancangan Sistem

3. HASIL DAN PEMBAHASAN

Studi ini melibatkan koneksi beberapa komputer, termasuk komputer server, komputer klien (client), dan komputer penyerang (attacker). Komputer server telah dipasang perangkat lunak SNORT, yang berperan dalam menangkap paket data yang menuju ke server tersebut. Di sisi lain, komputer penyerang telah dilengkapi dengan perangkat lunak hping3 untuk melancarkan serangan DDOS Attack terhadap server. Koneksi antara semua komputer ini diatur melalui sebuah switch. Berikut adalah langkah-langkah yang dijalankan dalam penelitian ini.

1. Instalasi Jaringan

   Dalam penelitian ini, digunakanlah jaringan lokal yang terdiri dari satu komputer server, satu komputer penyerang, dan satu komputer klien. Setiap komputer ini memiliki alamat IP sebagai berikut:

   - Server : 10.100.3.147
   - Client : 10.100.4.88
   - Attacker : 10.100.6.77

2. Installasi Snort

   Perangkat lunak SNORT telah dipasang di komputer server dengan tujuan membaca paket data yang ditujukan ke server tersebut. Aplikasi SNORT tersedia untuk diunduh dari situs web resmi https://www.snort.org/downloads. Pengguna diharuskan mengunduh perangkat lunak SNORT beserta aturannya (rules) dari situs tersebut.

   Setelah proses instalasi SNORT selesai, langkah berikutnya adalah melakukan konfigurasi SNORT agar dapat melakukan penangkapan paket data yang menuju ke komputer server. Dalam konfigurasi ini, pengguna harus menambahkan direktori ke dalam aturan (rules) SNORT agar SNORT dapat membedakan apakah paket data yang tiba di komputer server merupakan paket yang berpotensi berbahaya atau tidak. Beberapa aspek yang perlu dikonfigurasi meliputi:

   - Mengatur alamat IP untuk memungkinkan pemantauan lalu lintas jaringan dan mengonfigurasi direktori rules untuk memungkinkan membaca rules yang ada dalam SNORT.

     Konfigurasi IP address pada snort:

     1. var HOME_NET 10.100.0.254/16
     2. var EXTERNAL_NET !$HOME_NET
     3. var RULE_PATH c:\Snort\rules
     4. var PREPROC_RULE_PATH c:\Snort\preproc_rules
     5. var WHITE_LIST_PATH c:\Snort\rules
     6. var BLACK_LIST_PATH c:\Snort\rules
   - Untuk memungkinkan server mendeteksi intrusi, diperlukan penambahan aturan pada berkas local.rules.

     Membuat aturan yang akan dibaca oleh SNORT:

     1. alert icmp any any -> $HOME_NET any (msg:"PING to Server!!!!!"; sid:1000001;)
     2. alert tcp any any -> $HOME_NET any (msg:"Possible DoS Attack”; flags: S; flow:stateless; detection_filter:track by_dst, count 100, seconds 10; sid:1000002;)

   Pada tahap ini, pengguna dapat menyimpan intrusi yang telah terdeteksi dengan menyimpan file yang telah diinputkan.

   - Mengaktifkan Server Snort

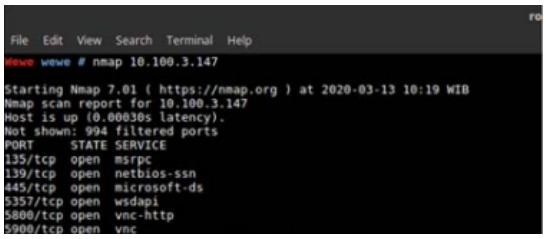
     Setelah menyelesaikan konfigurasi SNORT, SNORT perlu dijalankan agar dapat memantau paket-paket yang sedang mengarah ke computer server.

3. Ddos Attack

Komputer penyerang akan mencoba melaksanakan serangan DDOS Attack ke server SNORT dengan metode Pingfloodattack. Pingfloodattack adalah metode penyerangan yang melibatkan pengiriman sejumlah besar paket data dalam waktu singkat, yang dapat menyebabkan komputer target mengalami gangguan bahkan kerusakan[10]. Metode ini juga dapat menghambat kemampuan komputer target untuk berbagi file atau data dengan komputer lainnya. Dalam eksperimen ini, penyerang dengan alamat IP 10.100.6.77 mencoba melaksanakan Pingfloodattack terhadap server komputer yang memiliki alamat IP 10.100.3.147.

Dalam penelitian ini, sistem operasi Linux digunakan untuk menjalankan serangan DDOS Attack dengan aplikasi "hping3". Sebelum melancarkan serangan DDOS, pengguna pertama-tama melakukan pemindaian port dari komputer penyerang dengan aplikasi "nmap". Untuk menjalankan pemindaian port, langkah-langkah dapat dilakukan dengan perintah berikut:

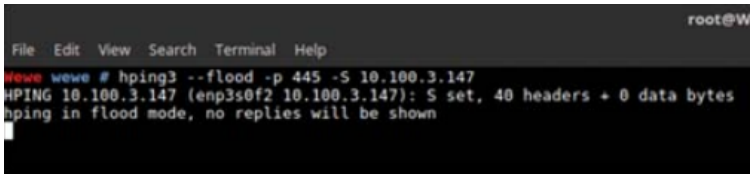
- Melakukan Port scanning
  1.Nmap 10.100.3.147



Gambar 4. Melakukan *Port Scaning* menggunakan Nmap

Setelah menyelesaikan pemindaian port, pada Gambar 4 terdapat beberapa port yang terbuka di PC server, termasuk port 135/tcp, 139/tcp, 445/tcp, dan sebagainya. Port-port ini dapat dijadikan sebagai titik masuk untuk melaksanakan serangan.

- Melakukan *Pingflood*
  Hping3 --flood -p 445 -S 10.100.3.147

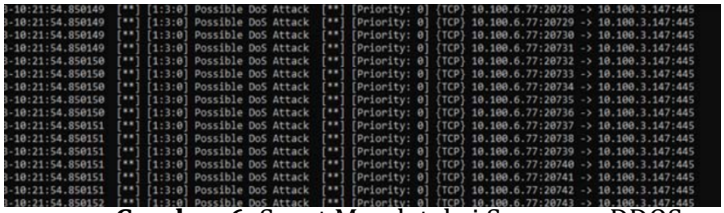


Gambar 5. Melakukan *pingflood*

Pada gambar 5 Penyerang menjalankan Pingflood dengan memanfaatkan port terbuka, yakni port 445.

- Hping3 adalah untuk menjalankan aplikasi Pingflood
- flood adalah perintah untuk mengalirkan lalu lintas data secara berlebihan.
- p 445 merujuk pada port yang akan menjadi target, yaitu port 445.
- S 10.100.3.147 adalah alamat IP yang akan menjadi sasaran serangan, yakni 10.100.3.147.

- Snort dapat mendeteksi serangan Ddos
  SNORT juga mampu mendeteksi informasi seperti waktu serangan, port yang menjadi sasaran, dan alamat IP penyerang pada komputer server.



Gambar 6. Snort Mendeteksi Serangan DDOS

Tabel 1. Hasil pengujian Dengan DDos Dengan IDS Snort

Pengujian	Sebelum	Sesudah
Ping (ICMP)	*205 byte/s*	*418 bytes/s*
Nmap	*205 bytes/s*	*48,0 kib/s*
DDoS	*205 bytes/s*	*80.mb/s*

Dari hasil penerapan intrusion Detection System dengan menggunakan snort untuk jaringan, hasil yang didapatkan dari penerapan snort, snort mampu mendeteksi adanya serangan seperti Ping (ICMP), Nmap dan DDOS yang masuk ke dalam jaringan komputer dengan memberikan sebuah alert atau informasi bahwa ada serangan yang masuk dengan informasi, tanggal dan waktu, type serangan,

4. KESIMPULAN

Berdasarkan hasil penelitian ini, dapat ditarik kesimpulan bahwa penerapan aplikasi SNORT dapat mendeteksi serangan-serangan jaringan melalui icmp, nmap, dan ddos. Metode intrusion Detection System adalah metode yang bisa mengoptimalkan tingkat keamanan jaringan komputer melalui pendeteksian serangan sehingga administrator jaringan dapat melakukan Tindakan pencegahan lebih awal.

DAFTAR PUSTAKA

[1] Asosiasi Penyelenggara Jasa Internet Indonesia." Accessed: Jul. 20, 2023. [Online]. Available: https://apjii.or.id/berita/d/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang
[2] daon001, "Polri: Indonesia Tertinggi Kedua Kejahatan Siber di Dunia."
[3] ari muach, "Apa Itu RT/RW-Net ," kompasiana.com.
[4] Barany Fachri and Fadli Hamdi Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *JURNAL MEDIA INFORMATIKA BUDIDARMA* , vol. 4, pp. 413–420, Apr. 2020.
[5] wikipedia, "Sistem deteksi intrusi," https://id.wikipedia.org/wiki/.
[6] ensiklopedia dunia, "Sistem deteksi intrusi ," https://p2k.stekom.ac.id/ensiklopedia/Sistem_deteksi_intrusi.
[7] S. S. M. K. Ade Heryana, "Informan dan Pemilihan Informan pada Penelitian Kualitatif," *Prodi Kesehatan Masyarakat – Universitas Esa Unggul*.
[8] Elsa Stephani and Fitri Nova, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," *jurnal ilmiah teknologi sistem informasi*, vol. 1, pp. 67–74, Jun. 2020.
[9] M Jafar Noor Yudianto, "Jaringan Komputer Dan Pengertiannya," *Komunitas eLearning IlmuKomputer.Com*, p. 8, 2007.
[10] Winrou Wesley Purba and Rissal Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT ," *Jurnal Teknologi Informas*, vol. 17, no. 2, pp. 143–158, Aug. 2020.