JIIFKOM (Jurnal Ilmiah Informatika & Komputer) STTR Cepu
E-Mail: jiifkom@sttrcepu.ac.id

Analisis Serangan dan Keamanan pada *Denial of Service (DOS)*: Sebuah Review Sistematik

Covinia Dinda Berliana[1], Teguh Adi Saputra[2], Indra Gunawan[3*]

Jurusan Teknik Elektro Sekolah Tinggi Teknologi Ronggolawe [12]
Jurusan Informatika Sekolah Tinggi Teknologi Ronggolawe [3]

[*]Email: igunsttr@gmail.com

Tentang naskah:
-diterima, 14 Jun 2022
-direview, 27 Jun 2022
-diterbitkan, 1 Jul 2022

Kata kunci: Denial of Service; Analisis; Review Sistematik

Intisari

Ancaman atau serangan pada jaringan atau system informasi dapat menyebabkan penyalahgunaan suatu informasi dalam kinerja organisasi. Salah satu ancaman atau serangan pada keamanan jaringan atau system informasi adalah Denial of Service (DoS). Risiko kehilangan asset informasi pada organisasi bisa terjadi jika tanda adanya perlindungan yang memadai. Teknologi keamanan yang sesuai dapat ditetapkan sebagai antisipasi dan perlindungan dari serangan DoS, maka diperlukan pemetaan terlebih dahulu antara jenis ancaman atau serangan dengan teknologi keamanan yang ada berdasarkan aspek kerahasiaan (confidentiality). Fail2ban, Wireshark, SDMD, Intrusion Dectetion System (IDS), dan Firewall menjadi teknologi keamanan pilihan dalam mengantisipasi dan melindungi jaringan atau system informasi pada aspek keamanan

Keyword: *Denial of Service; Analysis; Systematic Review*

Abstract

Threats or attacks on networks or information systems can cause misuse of information in organizational performance. One of the threats or attacks on network security or information systems is Denial of Service (DoS). The risk of losing information assets to the organization can occur if there are signs of adequate protection. Appropriate security technology can be set as anticipation and protection from DoS attacks, it is necessary to map in advance between the types of threats or attacks with existing security technologies based on the aspect of confidentiality. Fail2ban, Wireshark, SDMD, Intrusion Detection System (IDS), and Firewalls are the security technologies of choice in anticipating and protecting networks or information systems in security aspects

1. Pendahuluan

Perkembangan web site di dunia saat ini menyebabkan meningkatnya pengiriman information dan informasi secara international, selain didapatkan manfaat yang tinggi tentu saja resiko dan ancamannya juga semakin tinggi. Tanpa perlindungan tentu saja menyebabkan resiko ancaman menjadi lebih besar, Organisasi menjadi lebih rentan dalam menghadapai resiko ancaman dan serangan siber(Muhamad Dody Firmansyah 2021).

Resiko ancaman dan serangan keamanan terhadap suatu sistem dapat terjadi melalui tiga aspek keutuhan(integrity), kerahasiaan(confidentiality) serta ketersediaan(availability). Maka penting sebuah sistem berbasis digital diamankan terhadap tiga hal tersebut (Gunawan, 2021).

Saat ini terdapat banyak aplikasi berbasis web, yang mempermudah untuk memproses suatu data pada jaringan web. Oleh karena itu, peretas dapat dengan mudah bisa melakukukan serangan dengan leluasa (Mangapul Siahaan 2021).

Menurut laporan McAfee Labs Threts Report tahun 2018-2019, mayoritas serangan siber dilakukan dengan memanfaatkan celah-celah pada perangkat jaringan yang digunakan. Teknik dan metode serangan yang dilakukan pun bermacam-macam beberapa di antaranya adalah Denial of Service (DOS) dan (Lubi Arsada dan Aries Muslim 2021).

DoS adalah sebuah sistem penyerangan dimana peretas dapat melumpuhkan sistem target yang mengakibatkan dampak dalam sebuah sistem, hingga memiliki dampak tidak berjalannya sistem bahkan sampai merusak piranti keras(Farid Muhammad, Ida Wahidah, dan Arif Indra Irawan 2021).

Maka dapat dipahami bahwa tidak ada mekanisme atau metode yang dapat dilakukan untuk menghalangi secara menyeluruh dan pasti akan sebuah serangan DoS, namun sistem yang sudah dipersiapkan akan memiliki kemungkinan down time /ketidaktersediaan data yang lebih kecil dan kesempatan yang lebih baik (Joko Christian Chandra 2021) Dengan demikian, penelitian ini bertujuan untuk melakukan systematic review atas studi-studi tentang Denial of Service (DoS), Systematic review ini tidak memberikan opini suatu analisa melaikan hanya mengelompokan dan membandingkan metode keamanan dalam menghadapi DoS.

2. Kerangka Teori

Penelitian-penelitian yang kami kumpulkan berasal dari google schoolar yang bisa diakses di web dan bisa didapatkan tanpa adanya persyaratan. Selain itu penulis juga melihat referensi yang ada di penelitian tersebut.

2.1. Pemilihan Studi

1) Pencarian kata kunci, dipilih sesuai dengan minat penelitian penulis dalam meninjau serangan Denial of Service (DoS) yang sesuai sebagai metode perlindungannya. Kata kunci yang digunakan dalam pencarian penelitian pada database yang disebutkan yaitu;" Keamanan Informasi", "Ancaman Informasi", "Denial of Service", "Ancaman Kerahasiaan".

2) Eksplorasi dan pemilihan judul, abstrak, dan kata kunci dari penelitian-penelitian yang diidentifikasi dilakukan berdasarkan kriteria kelayakan.

3) Pembacaan lengkap atau sebagian penelitian yang memenuhi kriteria kelayakan dilakukan untuk menentukan apakah penelitian tersebut layak masuk dalam tinjauan.

4) Daftar referensi penelitian ditelaah untuk menemukan studi yang relevan.

2.2. Pengumpulan Data

Pengumpulan data dilakukan secara manual menggunakan instrumen tabel ekstraksi data yang terdiri dari: judul, penulis, tahun, nama jurnal/konferensi, tipe penelitian, topik, metode penelitian, hasil pembahasan dan kesimpulan. Penelitian yang relevan atau berpotensi relevan dinilai secara bersama-sama. Penilaian terdiri dari membaca teks lengkap dan data yang diekstrasi. Setiap perbedaan diselesaikan melalui diskusi antara penulis.

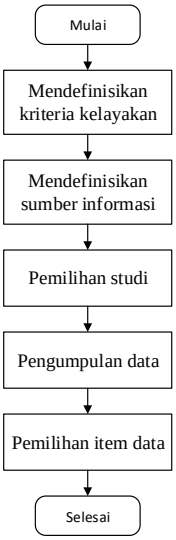
2.3. Pemilihan Item Data

Informasi yang diambil dari setiap penelitian terdiri dari:

1) Ancaman serangan Denial of Service; 2) Ancaman atau serangan kerahasiaan; 3) Metode keamanan yang ada sebagai perlindungan DoS.

3. Metodologi

Terdapat beberapa langkah dalam penelitian ini sesuai dengan pedoman yaitu;



Gambar 1. 1 Metodologi Penelitian

4. Hasil dan Pembahasan

4.1 Seleksi Penelitian

Hasil pencarian dalam *database* yang dipilih memberikan total 10 penelitian yang ditulis dalam bahasa Indonesia dari tahun 2019 hingga 2021, cocok dengan kata kunci yang perlu dianalisis. Akhirnya terpilih 6 penelitian yang memenuhi kriteria kelayakan dan menjadi bahan dalam review sistematik ini ini.

4.2 Karakteristik Penelitian

Informasi detil dari 6 *penelitian* yang terpilih dapat dilihat pada Tabel 1 tentang ekstrasi data final. Ekstrasi data final ini adalah tabel ekstrasi data yang hanya berisi *penelitian-penelitian* terpilih berdasarkan kriteria-kriteria yang ada pada proses seleksi *penelitian*.

Table 1.1 Ekstrasi Data Final

No	Penulis	Nama Jurnal/Konferensi	Tipe Penelitian	Topik	Metode	Hasil Pembahasan	Kesimpulan
1.	Mangapu l Siahaan , 2021	Jurnal Ilmu Penget ahuan dan Teknolo gi	Research Penelitian	Serangan DDoS terha dap Email Server	Kualitatif	Serangan : • Serangan DoS pada Email Teknologi : • Fail2ban	Pencegahan serangan DDoS diatasi dengan melakukan pemasangan aplikasi fail2ban
2.	Lubi & Aries, 20 21	Jurnal Ilmiah KOM PUTASI	Review Penelitian	Serangan DoS pada perangkat Internet of Things (IoT)	Kualitatif	Serangan : • Low Orbit Ion Cannon (LOIC) Teknologi : • Wireshark	Aplikasi wireshark dapat mengidentifikasi adanya serangan flooding
3.	Joko, 20 21		Research Penelitian	Serangan DoS pada s ystem E-Learning	Kualitatif	Serangan : • Volume based attack	Model framework digunakan sebagai acuan
4.	Jodi, Dany, Adhitya, 2019	Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer	Research Penelitian	Serangan menggunakan Classifier Dos	Kualitatif	Serangan : • Syn flooding • Udp flooding • Icmp flooding Teknologi: • SDMD	Kinerja SDMD dalam melakukan deteksi serangan sangat baik, semua akurasi yang didapatkan di atas 90%
5.	Farid, Ida & Arif,2021		Research Penelitian	Serangan DoS pada Jaringan Internet of Things (IoT)	Kualitatif	Serangan : • Communication nodes • Kanal komunikasi Teknologi : • Intrusion Dectetion System (IDS)	Pendektesian dengan synthetic network masih belum dapat dibilang akurat dalam pendeteksian

6.	Dody, 2021		Research Penelitian	Serangan DDoS pada Web Server	Kualitatif	Serangan : • CrossSite Scripting • Sql Injection • Phising Attack • Ddos Teknologi: • Firewall	Penyimpanan Data harus dalam bentuk yang sangat protektif

5. Simpulan

Dari penelitian tentang systematic review terkait dengan serangan dan tindak keamanan pada Denial of Service (Dos), maka penulis menyimpulkan bahwa teknologi keamanan yang sesuai dapat ditetapkan sebagai antisipasi dan perlindungan dari berbagai macam serangan DoS, maka diperlukan pemetaan terlebih dahulu antara jenis ancaman atau serangan dengan teknologi keamanan yang ada berdasarkan aspek kerahasiaan (confidentiality). Dengan demikian pemilihan teknologi keamanan sesuai yang dapat dilakukan serta dapat mengurangi beban biaya dikarenakan tersedianya teknologi yang memiliki berbagai macam seperti Fail2ban, Wireshark, SDMD, Intrusion Dectetion System (IDS), dan Firewall.

Daftar Pustaka

Gunawan, I. (2021). *Keamanan Data: Teori dan Implementasi*. Sukabumi: Jejak Publisher.

Muhammad, F., Wahidah, I. and Irawan, A.I., 2021. Analisis Pendeteksian Serangan Denial Of Service (dos) Menggunakan Logika Fuzzy Metode Mamdani Pada Jaringan Internet Of Things (iot). *eProceedings of Engineering*, *8*(1). Diunduh dari: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/download/14259/14043.

Sihombing, J.C.J., Kartikasari, D.P. and Bhawiyuga, A., 2019. Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software-Defined Network (SDN). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, *2548*, p.964X. Diunduh dari: http://jptiik.ub.ac.id/index.php/jptiik/article/view/6476.

Chandra, J.C., 2021. Model framework untuk analisis keamanan dari serangan denial of service pada sistem e-learning universitas budi luhur. Diunduh dari: https://www.unisbank.ac.id/ojs/index.php/sendi_u/article/view/8623.

Arsada, L. and Muslim, A., 2021. Penerapan Metode NIST untuk Analisis Serangan Denial of Service (DOS) pada Perangkat Internet of Things (IoT). *Jurnal Ilmiah KOMPUTASI*, *20*(2),pp.275-282. Diunduh dari: https://ejournal.jakstik.ac.id/index.php/komputasi/article/view/2724.

Siahaan, M., 2021. Mencegah serangan ddos (distributed denial of service) terhadap email server. *Science Tech: Jurnal Ilmu Pengetahuan dan Teknologi*, *7*(2), pp.13-21. Diunduh dari https://jurnal.ustjogja.ac.id/index.php/scienctech/article/view/9656.

Firmansyah, M.D., 2021. Analisa Keamanan Web Server Terhadap Serangan Distributed Denial of Service Menggunakan Modevasive. *Telcomatics*, *6*(1), pp.11-16. Diunduh https://journal.uib.ac.id/index.php/telcomatics/article/view/4990.