Journal of Internet and Software Engineering Vol: 1, No 4, 2024, Page: 1-7

Implementasi Serangan *Website Nextcloud* menggunakan DoS Beserta Pencegahannya

Cindy Arditha Claudia Manurung*, Mahatmadi Ariq Mayangkara, Muhamad Al Habsy, Shelvie Nidya Neyman

Teknologi Rekayasa Komputer, Sekolah Vokasi, Universitas IPB

Abstrak: *Nextcloud* adalah platform penyimpanan awan yang memungkinkan kolaborasi dan penyimpanan data yang aman. Namun, seperti layanan berbasis Internet lainnya, *Nextcloud* rentan terhadap serangan penolakan layanan *Denial of Service* (DoS), yang dapat memengaruhi ketersediaan layanan. Menerapkan langkah-langkah keamanan untuk melindungi *Nextcloud* dari serangan DoS penting untuk memastikan integritas dan ketersediaan data. Penelitian ini menjelaskan implementasi *firewall* sebagai pertahanan terhadap serangan DoS di *Nextcloud*. *Firewall* memungkinkan untuk memantau dan memfilter lalu lintas jaringan untuk mengidentifikasi dan memblokir permintaan yang mencurigakan atau berlebihan. Hasil pengujian menunjukkan bahwa penggunaan *firewall* secara signifikan mengurangi dampak serangan DoS pada *Nextcloud*, sehingga meningkatkan keandalan dan ketersediaan layanan.

Kata Kunci: DoS, Keamanan Siber, Penyimpanan Awan

DOI: https://doi.org/10.47134/pjise.v1i4.2640
*Correspondence: Cindy Arditha Claudia Manurung
Email: cindyyclaudia@apps.ipb.ac.id

Received: 01-08-2024
Accepted: 15-09-2024
Published: 31-10-2024

Abstract: *Nextcloud may be a cloud capacity stage that empowers secure information collaboration and capacity. Be that as it may, like other Internet-based administrations, Nextcloud is helpless to Refusal of Benefit (DoS) assaults, which can affect benefit accessibility. Actualizing security measures to secure Nextcloud from DoS assaults is vital to guarantee information astuteness and accessibility. This investigate depicts the usage of a firewall as a defense against DoS assaults on Nextcloud. The firewall permits for checking and sifting of arrange activity to recognize and square suspicious or over the top demands. Test comes about appear that the utilize of a firewall altogether diminishes the affect of DoS assaults on Nextcloud, subsequently upgrading benefit unwavering quality and accessibility.*

Keywords: *Cloud Storage, Cybersecurity, DoS*

Pendahuluan

Berkembangnya teknologi sangat berdampak pada kehidupan masyarakat Indonesia. Salah satu teknologi yang sangat penting dan digunakan oleh banyak masyarakat adalah penyimpanan awan atau *cloud storage* yang berguna untuk menyimpan data–data pribadi maupun yang bersifat publik. Untuk memenuhi kebutuhan terdapat beberapa media penyimpanan bersifat *open source* seperti *Nextcloud*. *Nextcloud* merupakan *open source* yang dirancang untuk layanan *cloud storage*, dengan *Nextcloud* pengguna dapat mengakses data melalui antarmuka web atau aplikasi client (Pada et al., 2023).

Dengan berkembangnya teknologi, keamanan teknologi juga menjadi hal yang penting saat ini. Banyak pengguna internet yang melakukan tindak kriminal seperti penyusupan dan penipuan yang dapat merugikan pengguna internet yang lain. Salah satu tindak kejahatan pada internet adalah DoS (*Denial of Services*). Serangan DoS bertujuan untuk membuat jaringan *router down* sehingga tidak mampu melayani permintaan user yang memiliki hak akses yang sah. Akibatnya akan mengganggu aktivitas operasional organisasi dan menimbulkan kerugian material maupun non material (Jaya et al., 2020).

Dalam penelitian ini penulis akan mencoba mengatasi serangan tersebut dengan menggunakan *firewall*. Menurut Fuji Hartono, *Firewall* merupakan sebuah sistem yang memberikan izin lalu lintas jaringan yang dianggap aman dalam melalui dan mencegah lalu lintas jaringan yang tidak aman (Arlis & Sahari, 2019).

Metode

Pada penelitian ini, penulis mempelajari konsep dasar dan berbagai jenis serangan *Denial of Service* (DoS), termasuk pemahaman tentang mekanisme serangan DoS dan dampaknya terhadap kinerja serta aksesibilitas situs *web Nextcloud*. Penulis juga meneliti peran *firewall* dalam melindungi situs *Nextcloud* dari serangan ini, yang menjadi dasar penting untuk memastikan bahwa langkah-langkah konfigurasi *firewall* yang diterapkan sesuai dengan kebutuhan perlindungan yang diinginkan.

Langkah pertama yang dilakukan adalah mempersiapkan server Ubuntu untuk dikonfigurasi dengan *firewall*. Pada tahap ini, penulis menggunakan *Uncomplicated Firewall* (UFW) sebagai alat konfigurasi *firewall*. Selain itu, penulis mengidentifikasi alamat IP dari penyerang dan server *Nextcloud* yang akan digunakan dalam proses konfigurasi dan pengujian.

Selanjutnya, penulis melakukan konfigurasi *firewall* untuk mengamankan situs *web Nextcloud* dari serangan DoS. Konfigurasi ini melibatkan pengaturan aturan *firewall* yang bertujuan untuk memblokir alamat IP yang mencurigakan atau yang teridentifikasi sebagai penyerang, dengan tujuan mencegah serangan DoS yang dapat mengganggu kinerja dan aksesibilitas situs *Nextcloud*.

Setelah konfigurasi *firewall* selesai, penulis melakukan percobaan dengan memantau log *firewall* untuk memastikan efektivitas *firewall* dalam mencegah serangan DoS. Penulis juga menggunakan alat nmap untuk menemukan *host* di jaringan komputer dengan mengirimkan paket dan menganalisis responsnya. Langkah ini penting untuk memastikan bahwa konfigurasi *firewall* berfungsi dengan baik dan mampu melindungi situs *Nextcloud* dari serangan yang berpotensi merusak.

Hasil dan Pembahasan

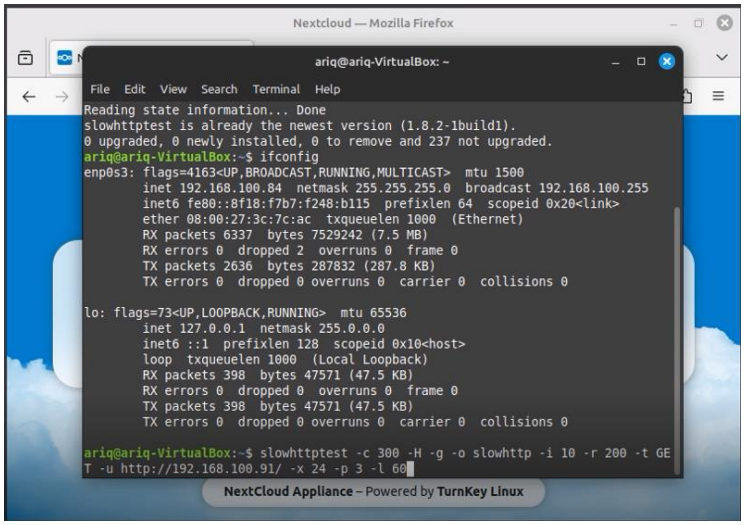
Penelitian terkait Serangan *Denial of Service* (DoS) pada website Nextcloud di Linux Mint ini bertujuan untuk membuat layanan tidak tersedia dengan membanjiri server menggunakan banyak permintaan secara bersamaan, sehingga server kewalahan dan tidak dapat merespons permintaan sah. Pencegahan dapat dilakukan dengan mengonfigurasi firewall di Linux Mint untuk memblokir lalu lintas mencurigakan, menggunakan load balancer untuk mendistribusikan beban secara merata, serta menginstal pembaruan rutin pada perangkat lunak Nextcloud dan sistem operasi untuk menutup celah keamanan.

Tabel 1. Spesifikasi OS pada VirtualBox

OS	Linux Mint	Debian
Versi	Linux Mint 21.3	Debian 11
RAM	2048 MB	2048 MB
CPU	2	8
Penyimpanan	25 GB	20 GB
Jaringan	Bridge Adapter	Bridge Adapter

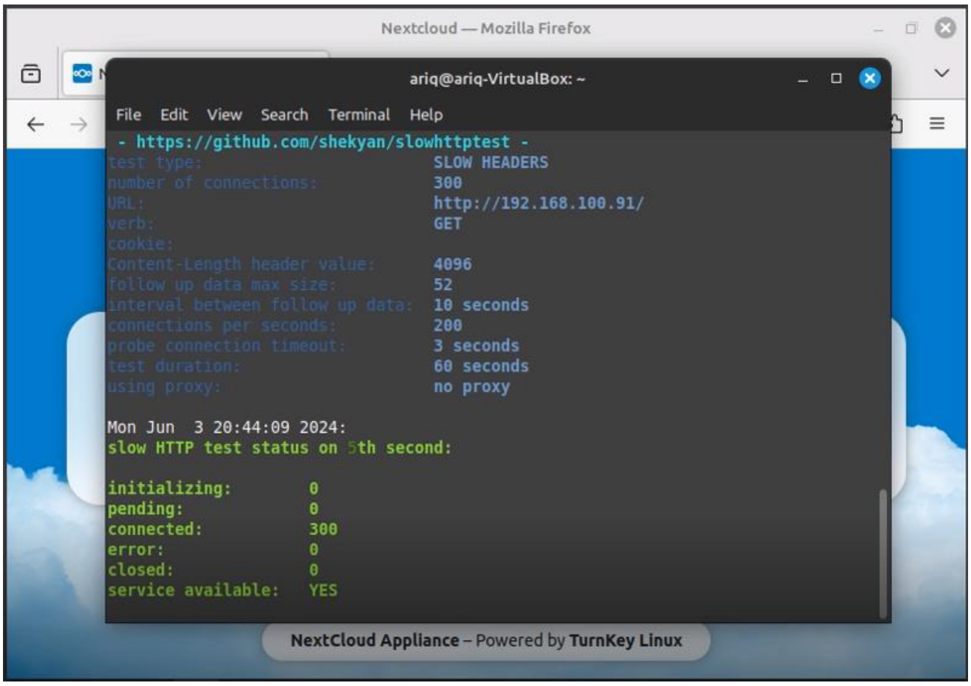
Pada tabel di atas, konfigurasi spesifikasi OS disusun untuk mesin virtual menggunakan VirtualBox. Konfigurasi tersebut mencakup beberapa aspek penting seperti Linux Mint dan Debian. Dengan menggunakan konfigurasi ini, mesin virtual Linux Mint apat dijalankan secara efisien dalam lingkungan VirtualBox, memungkinkan untuk pengujian penelitian ini dengan aman dan efektif (Purwoko et al, 2019).

Langkah pertama dalam melakukan penyerangan, kita akan memasukkan command pada cmd linux mint yaitu “slowhttptest -c 300 -H -g -o slowhttp -I 10 -r 200 -t GET -u http://192.168.100.91/ -x 24 -p 3 -l 60”.



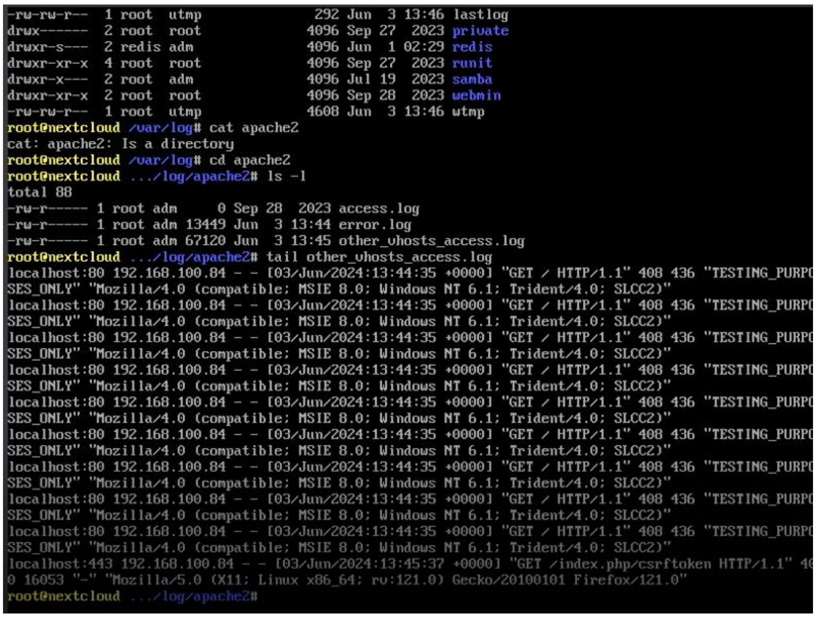
Gambar 1. Memasukkan Command pada Linux Mint untuk Melakukan Penyerangan

Setelah itu, pada gambar di bawah terlihat status connected 300 yang berarti serangan yang kita input telah berhasil memasuki website yang ingin kita serang.



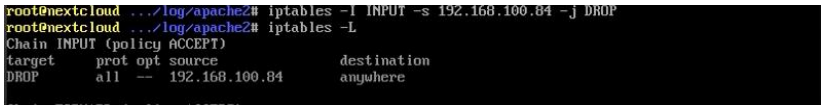
Gambar 2. Status Connected 300

Lalu untuk mengecek atau mengkonfirmasi serangan sudah masuk atau belum, kita bisa cek melalui *access log* pada *server cloud* dengan cara masuk ke direktori apache2 kemudian, masukkan command "tail other_vhost_access.log".



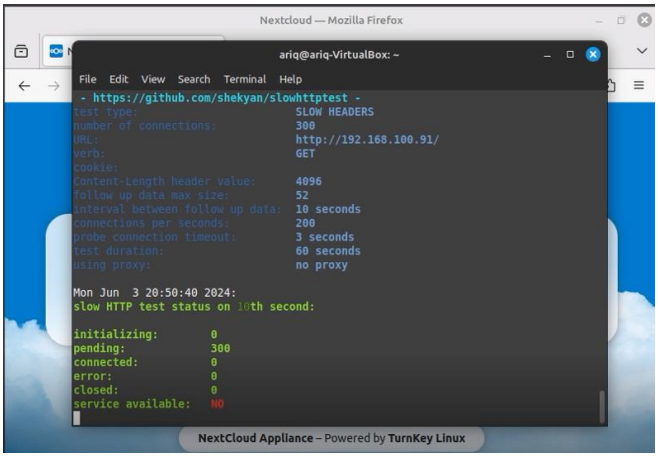
Gambar 3. Tampilan Access Log pada Server Cloud

Setelah kita berhasil menyerang, sekarang kita akan memitigasi atau mencegah penyerangan tersebut dengan cara memasukkan command "iptables -I INPUT -s 192.168.100.84 -j DROP" command tersebut berguna untuk menghentikan ip penyerang untuk mengakses dan menyerang kembali website kita.



Gambar 4. Menghentikan IP Penyerang untuk Kembali Mengakses Website

Pada saat penyerang kembali menyerang, gambar di bawah memperlihatkan perbedaan pada status connected yang menjadi 0 dan status pending menjadi 300, hal tersebut merupakan hasil dari mitigasi atau pencegahan yang telah dilakukan.



Gambar 5. Hasil Mitigasi Serangan yang Telah Dilakukan

Simpulan

Dalam penelitian ini, penulis berhasil menggunakan Linux Mint untuk melakukan serangan penolakan layanan (DoS) terhadap situs web Nextcloud dan mengembangkan langkah-langkah pencegahan yang efektif. Dengan mempelajari konsep dasar DoS dan kemungkinan jenis serangan, Anda dapat memahami bagaimana serangan ini dapat memengaruhi kinerja dan aksesibilitas situs Nextcloud Anda.

Pemahaman ini merupakan dasar penting untuk merancang dan menerapkan langkah-langkah mitigasi yang tepat. Penelitian telah menunjukkan bahwa firewall, khususnya *Uncomplication Firewall* (UFW) yang digunakan dalam sistem operasi Linux Mint, dapat secara signifikan mengurangi risiko serangan DoS.

Mengonfigurasi *firewall* Anda untuk memblokir alamat IP mencurigakan atau alamat IP yang diidentifikasi oleh penyerang dapat membantu menjaga kinerja dan aksesibilitas situs Nextcloud Anda. Menganalisis respons jaringan menggunakan alat nmap juga membuktikan bahwa *firewall* dapat mendeteksi dan memblokir lalu lintas yang tidak diinginkan, sehingga memastikan perlindungan sistem yang lebih baik.

Hasil eksperimen dan pemantauan log *firewall* menunjukkan bahwa tindakan pencegahan yang diterapkan bekerja dengan baik dalam melindungi situs Nextcloud dari serangan DoS. *Firewall* yang diterapkan dengan benar tidak hanya mengurangi risiko serangan, namun juga meningkatkan stabilitas dan keandalan layanan Nextcloud.

Studi ini menyoroti pentingnya konfigurasi *firewall* yang tepat dan pemantauan berkelanjutan untuk melindungi situs web dari ancaman dunia maya yang terus berkembang. Secara keseluruhan, pendekatan yang digunakan dalam penelitian ini dapat menjadi referensi untuk meningkatkan keamanan *website* serupa dari serangan DoS.

Daftar Pustaka

A. Cetinkaya, H. Ishii, and T. Hayakawa, "An overview on denial-of-service attacks in control systems: Attack models and security analyses," Entropy, vol. 21, no. 2, p. 210, Feb. 2019. doi:10.3390/e21020210

A. D. Sahara, S. Sapri, and A. A. Akbar, "The design and implementation of Computer Network Monitoring and Security System using linux ubuntu server," Jurnal Media Computer Science, vol. 3, no. 1, pp. 1–16, Jan. 2024. doi:10.37676/jmcs.v3i1.5328

Arwananing Tyas, Z., Firdonsyah, A., & Ramdhani, W. (2022). Analisis Keamanan Jaringan dari Serangan DoSpada Sistem Inventaris Sanggar Tari Natya Lakshita menggunakan IDS. Informatics Journal, 7(3), 258–267.

B. Jaya, Y. Yunus, and S. Sumijan, "Peningkatan Keamanan Router Mikrotik TERHADAP Serangan denial of service (dos)," Jurnal Sistim Informasi dan Teknologi, Sep. 2020. doi:10.37034/jsisfotek.v2i4.81

Fadhlillah, A. S., Nyoman Bogi, D. R., & Irawan, A. I. (2019). Analisis Performansi IDS Menggunakan Metode Deteksi Anomaly-Based Terhadap Serangan Dos. E-Proceeding of Engineering, 6(2), 3398–3405.

G. Fanani and I. Riadi, "Analysis of digital evidence on denial of service (dos) attack log based," Buletin Ilmiah Sarjana Teknik Elektro, vol. 2, no. 2, p. 70, Jul. 2020. doi:10.12928/biste.v2i2.1065

Halfond, W. G. J., & Orso, A. (2007). Detection and Prevention of *SQL Injection* Attacks. *Advances in Information Security*, *27*, 85–109. https://doi.org/10.1007/978-0-387-44599-1_5

Haris, A. I., Riyanto, B., Surachman, F., & Ramadhan, A. A. (2022). Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. Komputika: Jurnal Sistem Komputer, 11(1), 67–76. https://doi.org/10.34010/komputika.v11i1.5227

Irawan A., Sari A.P., Bahri S. (2019). Perancangan Dan Implementasi Cloud Storage Menggunakan Nextcloud. Jurnal Prosisko, vol. 5, no. 2, 131-143.

Khin SHAR, L., Beng Kuan TAN, H., Khin, L., & Beng Kuan, H. (2012). Defeating *SQL Injection* Defeating *SQL Injection* Part of the Information Security Commons, OS and Networks Commons, and the Programming Languages and Compilers Commons Citation Citation. *Defeating SQL Injection*, *46*(3), 69–77. https://ink.library.smu.edu.sg/sis_research/4898

M. Julda Alhafiz et al., "Dampak denial of service Pada Perusahaan Perbankan di Indonesia," Jurnal Ilmu Multidisplin, vol. 2, no. 1, pp. 114–120, Jun. 2023. doi:10.38035/jim.v2i1.233

Nabawi F., Susanto A.B., Mardiyanto. Perancangan Sistem Keamanan Server Linux Ubuntu 18.04 dengan Metode Ufw Firewall, Hardening, Chmod dan Chown pada UNUSIA Jakarta (2022). Jurnal Informatika Universitas Pamulang. 7(4), 808-818. doi: 10.32493/informatika.v7i2.22176

Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (2021). Ancaman dan Solusi Serangan Siber di Indonesia. Jurnal TECHNET: Telecommunications, Networks, Electronics, and Computer Technologies, 1(2), 86–92. http://ejournal.upi.edu/index.php/TELNECT/

Purwoko, M., & Hilal, H. (2019). Analisis Penerapan Firewall Nftables Sebagai Sistem Keamanan Server Pada Mesin Virtualisasi. Jurnal Telekomunikasi Dan Komputer, 9(1), 1–22. https://doi.org/10.22441/incomtech.v9i1.5676.

R. Shea and J. Liu, "Understanding the impact of denial of service attacks on Virtual Machines," 2012 IEEE 20th International Workshop on Quality of Service, Jun. 2012. doi:10.1109/iwqos.2012.6245975

Singh, P., Thevar, K., Shetty, P., & Shaikh, B. (2015). Detection of *SQL Injection* and XSS Vulnerability in Web Application. *International Journal of Engineering and Applied Sciences (IJEAS)*, *2*(3), 16–21. http://xyz.ac.in/departments/cse/csecourses.html

S. Sikkanan and Kasthuri M., "Denial-of-service and botnet analysis, detection, and mitigation," Research Anthology on Combating Denial-of-Service Attacks, pp. 20–48, 2021. doi:10.4018/978-1-7998-5348-0.ch002

Sumar, M.R., Wahid, A., Parenreng, J.M. (2024). Sistem Keamanan Jaringan Terhadap Serangan DOS (Denial Of Service) Menggunakan Snort Dan Firewall Berbasis Linux OS. Pinisi Journal of Science & Technology. 1(2).

W. B. Setiawan, E. Churniawan, and F. S. Faried, "Upaya regulasi Teknologi Informasi dalam Menghadapi Serangan Siber (cyber attack) Guna Menjaga Kedaulatan negara kesatuan Republik Indonesia," JURNAL USM LAW REVIEW, vol. 3, no. 2, p. 275, Dec. 2020. doi:10.26623/julr.v3i2.2773

Zhiyuan Tan, A. Jamdagni, Xiangjian He, P. Nanda, and Ren Ping Liu, "A system for denial-of-service attack detection based on multivariate correlation analysis," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 447–456, Feb. 2014. doi:10.1109/tpds.2013.146