Journal of Internet and Software Engineering Vol: 1, No 3, 2024, Page: 1-11

Perlindungan Keamanan *Website NextCloud*: Mengatasi Serangan DoS dengan Konfigurasi *Firewall* pada Ubuntu

Muhammad Rizky Alfazry*, Fikri Fadilah, Akhtarsyah Pambudi Putra, Aep Setiawan

Teknologi Rekayasa Komputer, Sekolah Vokasi, Institut Pertanian Bogor

Abstrak: Layanan *cloud* seperti *NextCloud* telah menjadi bagian penting dalam kehidupan digital, menawarkan fleksibilitas dan kemudahan akses data. Namun, layanan ini rentan terhadap serangan *Denial of Service* (DoS) yang dapat mengganggu kinerja dan aksesibilitas. Penelitian ini bertujuan untuk meningkatkan keamanan *NextCloud* dari serangan DoS dengan menggunakan konfigurasi *firewall* yang efektif. Simulasi serangan DoS dilakukan menggunakan slowhttptest pada server *NextCloud* yang diinstal pada Ubuntu. *Firewall* dikonfigurasi menggunakan iptables untuk memblokir paket dari sumber serangan. Hasil penelitian menunjukkan bahwa serangan DoS dapat membuat *website NextCloud* tidak dapat diakses atau sangat lambat. Dengan analisis log aktivitas server, *IP address* penyerang berhasil diidentifikasi dan diblokir. Pengujian ulang menunjukkan bahwa serangan berhasil dihentikan, membuktikan efektivitas konfigurasi *firewall* dalam mitigasi serangan DoS. Penelitian ini menyarankan pemantauan log secara rutin, penggunaan sistem deteksi dan pencegahan intrusi (IDS/IPS), dan pelatihan tim teknis dalam prosedur keamanan untuk meningkatkan perlindungan terhadap serangan DoS di masa depan.

Kata kunci: *DoS, Firewall, Nextcloud,* Keamanan*, Ubuntu*

DOI: https://doi.org/10.47134/pjise.v1i3.2639
*Correspondence: Muhammad Rizky Alfazry
Email: rizkyalfazry@apps.ipb.ac.id

Received: 15-05-2024
Accepted: 30-06-2024
Published: 31-07-2024

Abstract: *Cloud services such as NextCloud have become an essential part of digital life, offering flexibility and easy access to data. However, these services are vulnerable to Denial of Service (DoS) attacks that can disrupt performance and accessibility. This research aims to improve the security of NextCloud from DoS attacks by using an effective firewall configuration. DoS attack simulation is performed using slowhttptest on NextCloud server installed on Ubuntu. The firewall is configured using iptables to block packets from the attack source. The results show that DoS attacks can make the NextCloud website inaccessible or very slow. By analyzing the server activity logs, the attacker's IP address was identified and blocked. Retesting showed that the attack was successfully stopped, proving the effectiveness of firewall configuration in mitigating DoS attacks. This research suggests regular log monitoring, the use of intrusion detection and prevention systems (IDS/IPS), and training technical teams in security procedures to improve protection against future DoS attacks.*

Keywords: *Denial of Service, Firewall, Nextcloud, Securit, Ubuntu*

Pendahuluan

Pada masa kini, internet telah menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari manusia. Kemajuan teknologi informasi telah memberikan berbagai kemudahan, salah satunya melalui layanan cloud yang memungkinkan penyimpanan dan pengelolaan data secara efisien. Layanan *cloud* menjadi pilihan populer bagi individu maupun perusahaan karena fleksibilitas dan kemudahan akses yang ditawarkannya (Sumar et al., 2024).

Salah satu platform layanan *cloud* yang sering digunakan saat ini adalah *NextCloud*. *NextCloud* adalah solusi *open-source* yang memungkinkan pengguna untuk mengelola dan menyimpan data mereka secara mandiri dengan tingkat keamanan yang dapat disesuaikan (Marbun, 2021), Secara kegunaan *NextCloud* sama seperti layanan *cloud* pada umumnya seperti *Google Drive, DropBox*, dll (Marbun, 2021; Mayendra, 2021). Namun bedanya *NextCloud* merupakan jenis *private cloud* dimana pengguna harus menginstall sendiri pada server *private* yang membuat rentan terhadap serangan.

Penggunaan *cloud* yang setiap tahun mengalami peningkatan tentu tidak terhindar dari ancaman *cyberattack* yang juga naik setiap tahunnya. Menurut laporan survei yang dilakukan oleh SOPHOS dalam *whitepaper* "The State of Cloud Security 2020", tercatat sebanyak 70% dari 3.521 responden telah mengalami serangan pada *cloud* mereka (Tabrizchi & Rafsanjani, 2020). Praerit Grag dan Loren Kohnfelder dari Microsoft membagi jenis-jenis menjadi enam kategori yaitu *spoofing, tampering, repudiation, information disclosure, denial of service* (DoS), dan *elevation of privilage*. Yang mereka sebut sebagai STRIDE threat model (Mahjabin, 2018).

Kerentanan keamanan pada layanan *private cloud* dapat dimanfaatkan oleh penyerang untuk memberikan dampak kerugian kepada pihak pengguna, Salah satu jenis serangan yang dapat dilakukan terhadap layanan *cloud* adalah serangan *Denial of Service* (DoS), Dengan terjadinya serangan pada cloud data private dari pengguna dapat dengan mudah diakses oleh penyerang selain itu serangan pada layanan juga dapat mengakibatkan matinya akses dari layanan *cloud* yang dimiliki (Farry & Suartana, 2018).

Denial of Service atau biasa di sebut dengan DoS adalah jenis serangan yang biasanya menargetkan sebuah sistem layanan cloud dengan cara mengirimkan banyak http request dalam waktu bersamaan menggunakan sebuah komputer melewati internet. Lalu ada juga DDoS atau *Distibuted Denial of Sevice* yang merupakan versi lebih maju dari DoS yang dimana pada DDoS ini menggunakan beberapa komputer untuk melancarkan serangannya pada sebuah sistem (Farry & Suartana, 2018).

Meskipun ada banyak serangan yang lebih modern dari DoS pada kenyataannya jenis serangan DoS masih marak digunakan oleh penyerang untuk menyerang layanan sistem cloud di internet. Salah satu contohnya ialah serangan DDoS yang dilakukan kepada salah

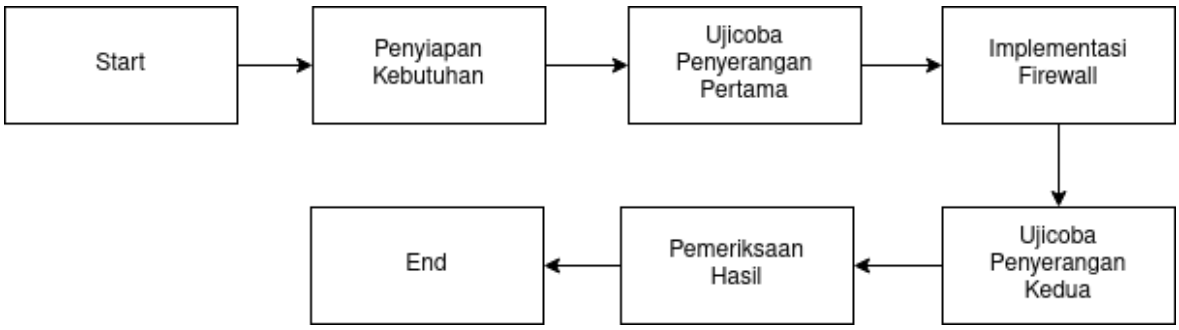
satu penyedia layanan *cloud* terbesar yaitu Microsoft Azure, dimana Microsoft Azure berhasil memitigasi serangan DDoS dengan skala besar yaitu 3.47 Tb/s dengan *packet rate* hingga 340 pps (Toh, 2021). Dengan maraknya serangan DoS yang terjadi pada layanan *Cloud* sudah menjadi kewajiban bagi pemilik layanan untuk menjaga layanan yang dimiliki, pada skala kecil seperti pemilik layanan *NextCloud* langkah awal yang dapat dilakukan untuk melakukan mitigasi serangan ini dapat berupa membuat sebuah *firewall* untuk filtrasi *packet* yang datang (Sudrajat, 2018).

Penggunaan *firewall* pada sebuah layanan jaringan *private cloud* dapat menjadi sebuah mitigasi minimal yang dapat di lakukan, *firewall* dapat melakukan filter terhadap *packet* yang akan masuk dan keluar dari sebuah sistem layanan *cloud* (Nimatul et al, 2020). Pada *private cloud* skala kecil penggunaan *firewall* yang gratis seperti *iptables* yang tersedia pada sistem operasi berbasis linux dapat menjadi pilihan utama karena dokumentasi yang tersebar menjadikan penggunaannya menjadi mudah di implementasikan.

Oleh karena itu tujuan dari dilakukannya penelitian ini adalah untuk melakukan ujicoba penyerangan sebuah *private cloud* dengan serangan DoS dan melakukan mitigasi serangan dengan membuat sebuah *firewall* yang akan memfilter *packet* yang akan masuk ke jaringan *cloud*. Untuk melihat keefektifan dari mitigasi yang di bentuk.

Metode

Dalam penelitian ini tahapan-tahapan penelitian dilakukan dengan beberapa tahap yang sudah di tentukan sebagai berikut



Gambar 1. Metode Penelitian

Pada gambar 1 dijelaskan bahwa tim penulis melakukan penyiapan kebutuhan penelitian seperti server *private cloud* (NextCloud) yang di *install* pada sebuah *virtual environment* (Sunaryo & Kasnawi, 2017). Yang nantinya akan di serang dengan DoS tanpa dan dengan implementasi *firewall* pada layanan *cloud*.

Dalam ujicoba kali ini kali linux akan digunakan sebagai *virtual machine* yang akan melakukan penyerangan DoS terhadap sebuah *NextCloud*. Sistem operasi ini memang dirancang khusus untuk melakukan kegiatan keamanan jaringan baik rekayasa jaringan, penetrasi, atau hal yang akan peneliti lakukan saat ini (Putri & Widyastuti, 2023).

Slowhttptest merupakan *tools* yang akan digunakan untuk melakukan serangan DoS ini (Sikora et al, 2021). Untuk *NextCloud* yang akan diserang terinstall pada jaringan yang sama dengan ip berbeda yang terinstal pada sebuah *virtual machine* Ubuntu (Ulfa et al, 2019).

Untuk sisi keamanannya server *nextcloud* membuat sebuah *firewall* yang akan memfilter *packet* yang akan masuk ke dalam jaringan (Wulandari, 2018). Jika paket tidak terdaftar pada rules yang di buat pada *firewall* maka *packet* akan di *drop* dan tidak diteruskan (Avinash, 2024).

Untuk *Firewall* yang akan digunakan adalah *iptables* (Mizan & Ibnu, 2018) yang merupakan *firewall* sederhana yang tersedia secara *default* pada mayoritas sistem operasi berbasis linux (Glen & Meicy, 2014) dengan penggunaan *iptables* ini layanan *cloud* akan menjadi lebih tahan terhadap serangan *Denial of Service* (DoS).

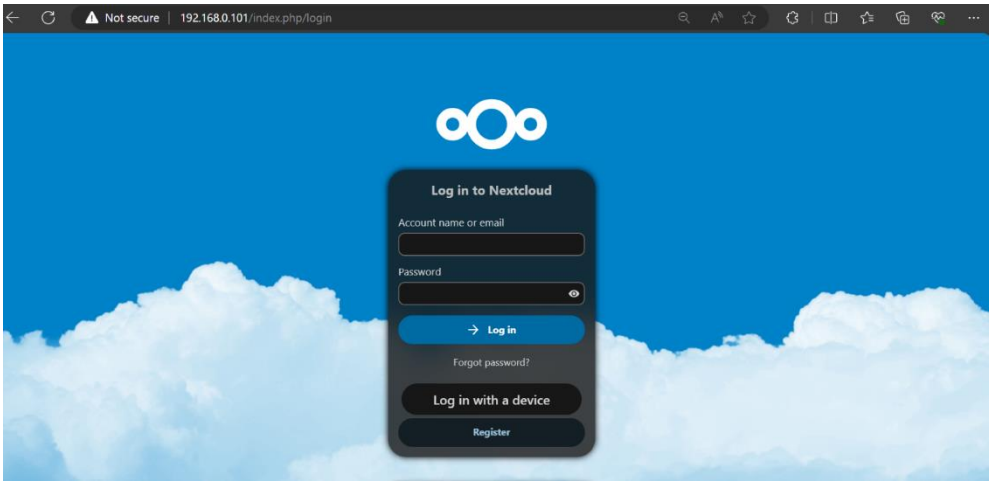
Hasil dan Pembahasan

Penelitian ini bertujuan untuk meningkatkan keamanan dari serangan DoS (Denial of Service) pada website nextcloud dengan menggunakan konfigurasi *Firewall* yang efektif. Selain itu, pada penelitian ini juga ditunjukkan bagaimana dampak serangan DoS (Denial of Service) pada *website nextcloud*. Untuk mencapai tujuan tersebut, ada beberapa Langkah yang harus dilakukan. Langkah yang pertama yaitu dengan menginstall OS Kali Linux dan juga Ubuntu sebagai server *website nextcloud*, yang digunakan untuk Simulasi Serangan DoS pada Server *website Nextcloud*.

Tabel 1. Spesifikasi Operating System

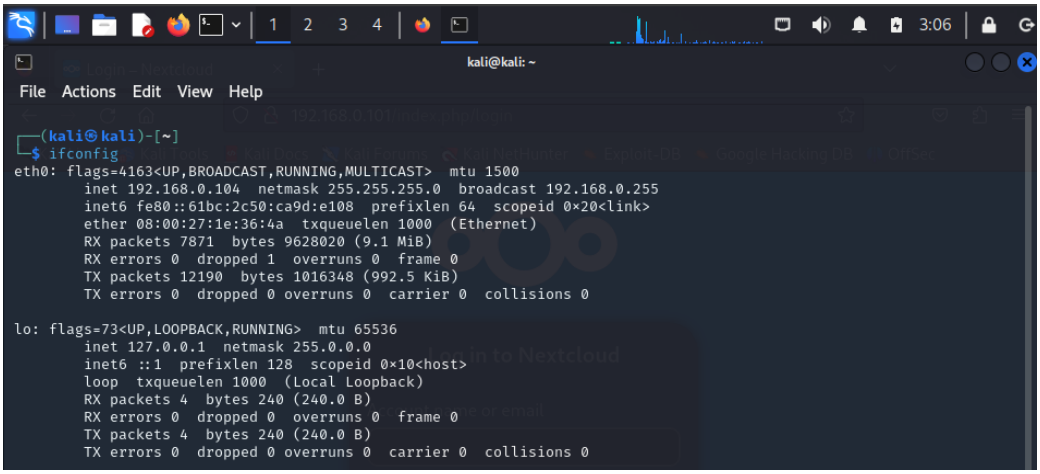
Spesifikasi	Kali Linux	Ubuntu Server
Versi	Kali Linux 2024.1 x64	Ubuntu Server 22.04.06 x64
RAM	2048 MB	4096 MB
CPU	2	2
Storage	80 GB	25 GB
Network	Bridge Adapter	Bridge Adapter

Dari tabel di atas, dapat diketahui spesifikasi dari masing-masing OS tersebut. Spesifikasi tersebut mencakup Versi dari OS itu sendiri, jumlah RAM yang digunakan, CPU, Media penyimpanan, serta jaringan yang digunakan. Dengan mengetahui spesifikasi dari masing-masing OS yang digunakan, dapat memudahkan penelitian ini agar lebih efisien.



Gambar 2. Website Nextcloud

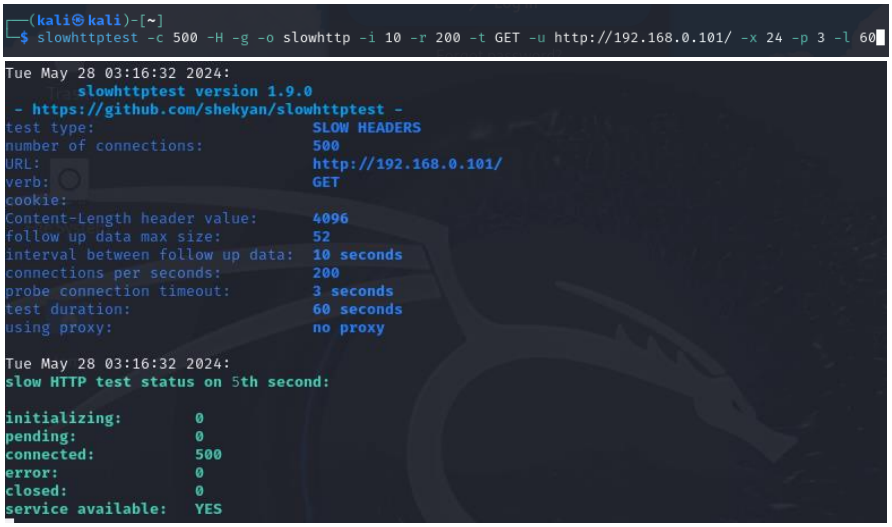
Setelah menginstall dua OS tersebut, pada bagian Ubuntu Server digunakan sebagai *website nextcloud*. Pada server *nextcloud* ini peneliti dapat mengetahui *IP Address* dari server tersebut yaitu 192.168.0.101. Pada ubuntu server ini juga yang nantinya akan dikonfigurasi *firewall* untuk mengatasi serangan DoS.



Gambar 3. IP Address Kali Linux

Sedangkan pada bagian Kali Linux, peneliti dapat mengetahui *IP Address* dari OS tersebut yaitu 192.168.0.104. Pada bagian Kali Linux ini nantinya akan digunakan sebagai simulasi untuk melakukan serangan DoS terhadap Server *nextcloud*. Untuk mengimplementasikan hal tersebut, peneliti menyusun langkah-langkahnya sebagai berikut:

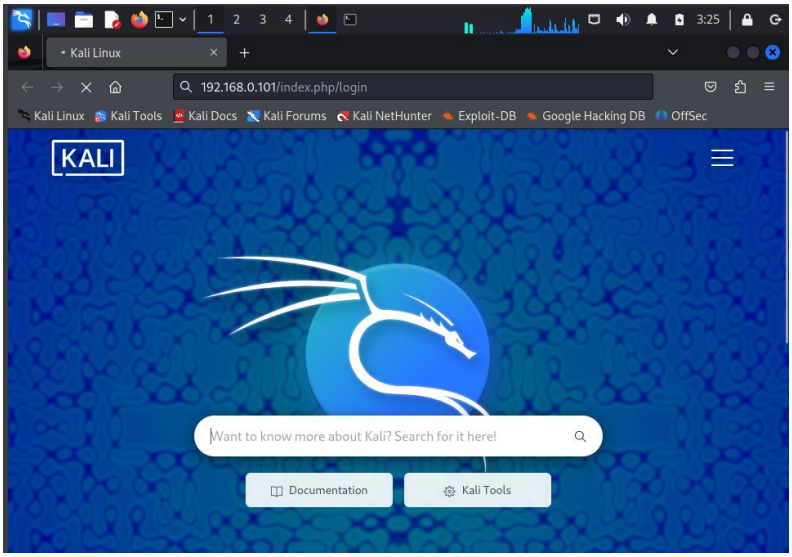
Simulasi Serangan DoS Menggunakan slowhttptest



Gambar 4. Simulasi Serangan DoS terhadap Website Nextcloud

Langkah pertama yaitu melakukan simulasi serangan DoS menggunakan *tools* slowhttptest. Untuk perintah yang digunakan yaitu "**slowhttptest -c 500 -H -g -o slowhttp -i 10 -r 200 -t GET -u http://192.168.0.101/ -x 24 -p 3 -l 60**". Perintah tersebut berfungsi untuk memberikan serangan lambat pada *IP Address* 192.168.0.101 yang merupakan IP Address dari server website nextcloud (Ramlan & Avinan, 2019). Pada perintah tersebut juga dilengkapi dengan beberapa parameter yaitu sebanyak 500 pesan yang dikirim serta 60 detik untuk durasi serangannya.

Mengakses *Website Nextcloud* dan Mendeteksi Serangan DoS



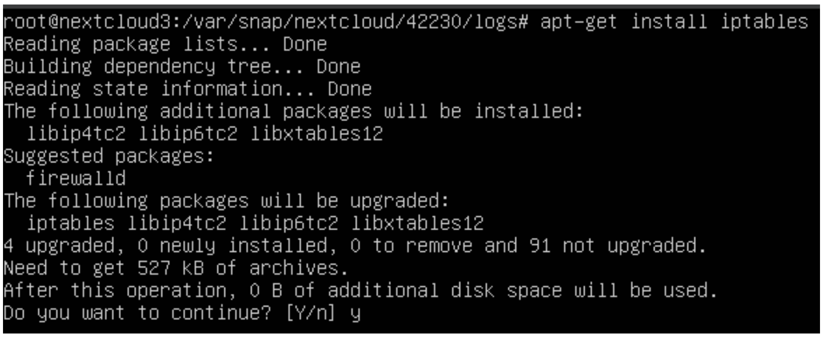
Gambar 5. Websiet Nextcloud terkena serangan DoS

Setelah melakukan simulasi serangan DoS, selanjutnya yaitu mengakses *website nextcloud* dengan IP Address 192.168.0.101 untuk melihat dampak yang diperoleh *website* tersebut setelah mengalami serangan DoS pada server nextcloudnya. Seperti gambar di atas, dampak dari serangan tersebut, *website nextcloud* tidak dapat di akses oleh siapapun dikarenakan banyak nya pesan HTTP yang tertuju pada *website* tersebut yang membuatnya tidak dapat diakses atau akses menjadi lambat. Dengan kondisi tersebut dapat diketahui bahwa serangan DoS sangat berdampak atau mempengaruhi kinerja dan juga mengganggu layanan *website* tersebut.

Gambar 6. Periksa Log Aktivitas server website

Untuk mengatasi serangan tersebut, yang pertama peneliti lakukan yaitu dengan memeriksa log aktivitas pada server *website* tersebut. *Log* aktivitas website tersebut berada pada direktori "/var/snap/nextcloud/42230/logs/". Kemudian gunakan perintah **tail -f apache_access.log** untuk memeriksa file access.log pada *website* tersebut (Darmawan, 2024). Setelah menjalankan perintah tersebut, peneliti dapat mengetahui *IP Address* dari penyerang yaitu 192.168.0.104 yang melakukan *spam* untuk memberikan pesan http terhadap *website* tersebut. Dengan melakukan analisis terhadap log aktivitas *website* ini memungkinkan peneliti dapat mengidentifikasi pelaku serangan serta jenis serangan yang diterima oleh *website* tersebut agar memudahkan peneliti untuk menangani berbagai serangan yang dihadapi.

Konfigurasi *Firewall* untuk Mengatasi Serangan DoS



```
root@nextcloud3:/var/snap/nextcloud/42230/logs# apt-get install iptables
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libip4tc2 libip6tc2 libxtables12
Suggested packages:
  firewalld
The following packages will be upgraded:
  iptables libip4tc2 libip6tc2 libxtables12
4 upgraded, 0 newly installed, 0 to remove and 91 not upgraded.
Need to get 527 kB of archives.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Gambar 7. Installasi iptables

Setelah memeriksa aktivitas log dari *website* dan mengetahui *IP Address* dari pelaku serangan, selanjutnya peneliti melakukan konfigurasi *firewall* dengan menggunakan iptables. Pertama, install terlebih dahulu iptables pada server *website* dengan menggunakan perintah **apt-get install iptables.**

```
root@nextcloud3:/var/snap/nextcloud/42230/logs# iptables -I INPUT -s 192.168.0.104 -j DROP
root@nextcloud3:/var/snap/nextcloud/42230/logs# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.0.104        anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Gambar 8. Blokir IP Address penyerang

Setelah menginstall iptables, gunakan perintah **iptables -I INPUT -s 192.168.0.104 -j DROP** untuk melakukan blokir pada *IP Address* pelaku serangan tadi (Rahman et al, 2020). Dengan menggunakan perintah tersebut, pelaku serangan sudah tidak bisa melakukan akses terhadap *website nextcloud* lagi. Selanjutnya, gunakan perintah **iptables -L** untuk20 melihat aturan yang digunakan sudah diterapkan dengan benar atau belum.

Memeriksa Hasil Konfigurasi *Firewall*

```
root@nextcloud3:/var/snap/nextcloud/42230/logs# tail -f apache_access.log
192.168.0.104 - - - [28/May/2024:07:38:08 +0000] "GET / HTTP/1.1" 400 392 "TESTING_PURPOSES_ONLY" "O
pera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition MacAppStore; en) Mozilla/5.0 (Macintosh; Int
el Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34"
192.168.0.104 - - - [28/May/2024:07:38:08 +0000] "GET / HTTP/1.1" 400 392 "TESTING_PURPOSES_ONLY" "O
pera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition MacAppStore; en) Mozilla/5.0 (Macintosh; Int
el Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34"
192.168.0.104 - - - [28/May/2024:07:38:08 +0000] "GET / HTTP/1.1" 400 392 "TESTING_PURPOSES_ONLY" "O
pera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition MacAppStore; en) Mozilla/5.0 (Macintosh; Int
el Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34"
192.168.0.104 - - - [28/May/2024:07:38:08 +0000] "GET / HTTP/1.1" 400 392 "TESTING_PURPOSES_ONLY" "O
pera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition MacAppStore; en) Mozilla/5.0 (Macintosh; Int
el Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34"
192.168.0.104 - - - [28/May/2024:07:38:08 +0000] "GET / HTTP/1.1" 400 392 "TESTING_PURPOSES_ONLY" "O
pera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition MacAppStore; en) Mozilla/5.0 (Macintosh; Int
el Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34"
192.168.0.104 - - - [28/May/2024:07:38:08 +0000] "GET / HTTP/1.1" 400 392 "TESTING_PURPOSES_ONLY" "O
pera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition MacAppStore; en) Mozilla/5.0 (Macintosh; Int
el Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34"
192.168.0.104 - - - [28/May/2024:07:38:08 +0000] "GET / HTTP/1.1" 400 392 "TESTING_PURPOSES_ONLY" "O
pera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition MacAppStore; en) Mozilla/5.0 (Macintosh; Int
el Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34"
192.168.0.104 - - - [28/May/2024:07:38:08 +0000] "GET / HTTP/1.1" 400 392 "TESTING_PURPOSES_ONLY" "O
pera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition MacAppStore; en) Mozilla/5.0 (Macintosh; Int
el Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34"
192.168.0.104 - - - [28/May/2024:07:38:08 +0000] "GET / HTTP/1.1" 400 392 "TESTING_PURPOSES_ONLY" "O
pera/9.80 (Macintosh; Intel Mac OS X 10.7.0; U; Edition MacAppStore; en) Mozilla/5.0 (Macintosh; Int
el Mac OS X) AppleWebKit/534.34 (KHTML,like Gecko) PhantomJS/1.9.0 (development) Safari/534.34"
192.168.0.104 - - - [28/May/2024:07:50:09 +0000] "GET /index.php/csrftoken HTTP/1.1" 200 925 "-" "Mo
zilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

Gambar 9. Periksa Kembali Log Aktivitas server website

Setelah melakukan konfigurasi *Firewall* pada server *website nextcloud*, selanjutnya periksa Kembali aktivitas *log* dari *website* untuk memastikan bahwa serangan DoS sudah terhenti. Dapat dilihat dari gambar diatas, bahwa serangan dari *IP Address* 192.168.0.104 sudah terhenti.

Gambar 10. Simulasi Kembali Serangan DoS terhadap Website Nextcloud

Untuk memastikannya, peneliti melakukan simulasi ulang untuk menyerang server *website* itu lagi. Dan dapat dilihat dari gambar diatas, bahwa pelaku serangan sudah tidak bisa melakukan serangan lagi terhadap server *website nextcloud*. Dengan hal ini menunjukkan bahwa penggunaan konfigurasi *Firewall* sudah berhasil dan terlihat dapat menghentikan serangan DoS.

Simpulan

Dari hasil penelitian ini dapat disimpulkan, bahwa serangan *Denial of Service* (DoS) dapat secara signifikan mengganggu kinerja dan aksesibilitas dari *website Nextcloud*. Selain itu, simulasi serangan menggunakan slowhttptest mengungkapkan bahwa serangan DoS dapat membuat *website* tidak dapat diakses atau sangat lambat diakses. Melalui pemeriksaan log aktivitas server, peneliti mampu mengidentifikasi *IP address* pelaku serangan dan memahami jenis serangan yang dilakukan. Dengan menerapkan konfigurasi firewall menggunakan iptables, akses dari IP address pelaku berhasil diblokir, sehingga serangan DoS dapat dihentikan. Pengujian ulang pasca-konfigurasi menunjukkan bahwa pelaku serangan tidak lagi mampu menyerang server, membuktikan efektivitas dari konfigurasi firewall dalam mengatasi serangan DoS.

Adapun beberapa saran dari penelitian ini yaitu yang pertama meningkatkan keamanan *website Nextcloud* dari serangan DoS di masa mendatang, pemantauan log aktivitas secara rutin dan analisis pola serangan sangat dianjurkan. Kedua, selain konfigurasi *firewall*, penggunaan keamanan tambahan seperti IDS/IPS dapat mendeteksi

dan mencegah berbagai jenis serangan. Ketiga, selalu perbarui sistem operasi, aplikasi *Nextcloud*, dan perangkat lunak keamanan dengan patch terbaru untuk menghindari eksploitasi kerentanan. Terakhir, penting untuk melatih tim teknis dalam prosedur keamanan dan penanganan insiden agar dapat merespons dengan cepat dan tepat saat terjadi serangan, memastikan layanan tetap tersedia dan andal bagi pengguna.

Daftar Pustaka

Avinash, K. (2024). Packet Filtering Firewalls (Linux). Purdue University. https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture18.pdf

Darmawan, D. (2024). Nextcloud: Keamanan Data Terbaik Dengan Manajemen File Dan Pengguna Yang Cerdas. Jurnal Sosial dan Teknologi (SOSTECH), 4(1), 2774-5147.

Farry, B., & Suartana, I. (2018). Deteksi Serangan Denial of Service (DoS) Pada Cloud Menggunakan Security Onion. JINACS, 5, 2686-2220.

Glen, S., & Meicy, I. (2014). Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat. E-journal Teknik Elektro dan Komputer, ISSN: 2301-8402.

Mahjabin, S. (2018). Implementation of DoS and DDoS Attacks on Cloud Servers. Period. Eng. Nat. Sci., 6(2), 148–158. doi: 10.21533/pen.v6i2.170.

Marbun, R., Fitri, I., & Iskandar, A. (2020). Nextcloud 2 Terabyte LAN Network-Based Server By Using the Ubuntu LTS 16.04. doi: 10.35335/cit.vol12.pp1-6.

Mayendra, L., Saputra, H., & Hasanah, U. (2021). Rancang Bangun Local Cloud Server Dengan NextCloud Pada Centos 7 Di SRH Training Center. doi:10.33330/jutsi.v1i1.1045.

Mizan, S., & Ibnu, F. (2016). Penerapan IPtables Firewall Pada Linux Dengan Menggunakan Fedora. Jurnal Manajemen Informatika, 6(1), 198-207.

Nimatul, M., Stefanus, E., & Abner, O. (2020). Rancangan Sistem Keamanan Jaringan dari Serangan DDoS Menggunakan Metode Pengujian Penetrasi. JTEKSIS, 6(1), 162-167.

Putri, Y., & Widyastuti. (2023). Perancangan Private Cloud Storage Menggunakan Nextcloud untuk Meningkatkan Kinerja Administrasi di Sekolah. https://repository.uksw.edu//handle/123456789/32266

Rahman, D. A., Syamsul, R. A., & Budi, S. (2020). Implementasi IPTables untuk Packet Filtering Firewall. Dielektrika, 6(1), 61-66.

Ramlan, T., & Avinan. (2019). Pemodelan HTTP Request dengan Regular Expression untuk Deteksi Serangan Slow HTTP DoS. Jurnal Pekommas, 4(1), 31-42.

Sikora, M., Fujdiak, R., & Kuchar, K. (2021). Generator of Slow Denial-of-Service Cyber Attacks. https://doi.org/10.3390/s21165473

Sudradjat, B. (2018). Sistem Pendeteksian Dan Pencegahan Penyusup Pada Jaringan Komputer Dengan Menggunakan Snort Dan Firewall. JISAMAR: Journal of Information System, Applied, Management, Accounting and Research, 1(1), 10-24.

Sumar, R., Wahid, J., & Parenreng. (2024). Sistem Keamanan Jaringan Terhadap Serangan DOS (Denial Of Service) Menggunakan Snort Dan Firewall Berbasis Linux OS. PINISI: Journal of Science and Technology, 1(1).
Sumar, R., Wahid, J., & Parenreng. (2024). Sistem Keamanan Jaringan Terhadap Serangan DOS (Denial Of Service) Menggunakan Snort Dan Firewall Berbasis Linux OS. PINISI: Journal of Science and Technology, 1(1).
Sunaryo, T., & Kasnawi. (2017). Rancang Bangun Server Cloud Computing Di Politeknik Negeri Bengkalis. JIPOLBENG - Informatika, 2(1).

Tabrizchi, H., & Rafsanjani, K. (2020). A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions. J. Supercomput., 76, 9493–9532.

Toh, A. (2021). Azure DDoS Protection-2021 Q3 and Q4 DDoS Attack Trends. 2022. https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q3-and-q4-ddos-attack-trends/

Ulfa, M., Panjaitan, F., & Suryayusra. (2019). Layanan Private Cloud Berbasis NextCloud pada SMKN 1 Indralaya Utara. Jurnal Pengabdi, 1(2), 2620-4673.

Wulandari, S. R. (2018). Implementasi Firewall pada Cloud Computing Dengan CSF. Pustaka Politeknik Pekanbaru. https://opac.lib.pcr.ac.id/index.php?p=fstream&fid=4397&bid=8306