IMPLEMENTASI *FIREWALL TARPIT* PADA *ROUTER* SEBAGAI PERLINDUNGAN TERHADAP SERANGAN *PORT SCANNING*

PROJEK

Sebagai Salah Satu Syarat Untuk Menyelesaikan Studi di
Program Studi Teknik Komputer DIII

Oleh:

Achmad Hasan

09030582125004

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

JULI 2024

HALAMAN PENGESAHAN

IMPLEMENTASI *FIREWALL TARPIT* PADA *ROUTER* SEBAGAI PERLINDUNGAN TERHADAP SERANGAN *PORT SCANNING*

PROJEK

Sebagai Salah Satu Syarat Untuk Menyelesaikan Studi di
Program Studi Teknik Komputer DIII

Oleh:

Achmad Hasan
0930582125004

Palembang, 29 Juli 2024

Menyetujui,

Pembimbing I	Pembimbing II
Adi Hermansyah, M.T.	**Nurul Afifah, M.Kom**
NIP. 198904302024211001	**NIP. 199211102023212049**

Mengetahui, 31/7/24

Plt. Koordinator Program Studi Teknik Komputer,

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : **Rabu**

Tanggal : **17 Juli 2024**

Tim Penguji :

1. Ketua Sidang : Ahmad Heryanto, M.T.
2. Penguji : Rahmat Fadli Isnanto, M.Sc.
3. Pembimbing I : Adi Hermansyah, MT
4. Pembimbing II : Nurul Afifah, M.Kom

Mengetahui,
Plt. Koordinator Program Studi Teknik Komputer,

Dr. Ir. Sukemi, M.T.
NIP 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Achmad Hasan

NIM : 09030582125004

Program Studi : Teknik Komputer

Judul Projek : Implementasi *Firewall Tarpit* Pada *Router* Sebagai Perlindungan Terhadap Serangan *Port Scanning*

Hasil Pengecekan iThenticate/Turnitin : 13%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari universitas sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.

Palembang, 17 Juli 2024

Achmad Hasan

NIM 09030582125004

HALAMAN PERSEMBAHAN

"Disiplin diri adalah sebenar-benarnya wujud kebebasan yang hakiki"

"Masa lalu saya adalah milik saya, Masa lalu kamu adalah milik kamu. Tapi, masa depan adalah milik kita". (B.J.Habibie)

"Janganlah kamu bersikap lemah dan janganlah pula kamu bersedih hati, padahal kamulah yang paling tinggi derajatnya jika kamu beriman".

(QS.Ali Imran [3]:139

Dengan mengucap syukur Alhamdulillah atas rahmat Allah

Subhanahu wa Ta'ala, kupersembahkan karya kecil ini untuk….

Kedua Orang tua tercinta

(Abi dan umi)

Saudara dan Saudariku

(Kak Latifah, Kak Fariza Hanum, Bang M.Syafiq,)

Teman-teman seperjuangan prodi,

(Teknik Komputer 2021)

Almamater perjuangan

(Universitas Sriwijaya)

Juli 2024

KATA PENGANTAR

Segala puji dan syukur atas kehadirat Allah Subhanahu wa Ta'la, karena berkat Rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penulisan projek akhir dengan judul "**Implementasi Firewall Tarpit Pada Router Sebagai Perlindungan Terhadap Serangan *Port scanning*"**. Penulisan projek akhir ini dibuat dalam rangka memenuhi syarat untuk menyelesaikan pendidikan di program studi Teknik Komputer Fakultas Ilmu Komputer Universitas Sriwijaya untuk memperoleh gelar Ahli Madya Komputer.

Pada kesempatan ini, penulis menyampaikan ucapan terima kasih kepada banyak pihak yang telah memberikan bantuan, dukungan dan saran secara moril dan materil kepada penulis sehingga terselesaikannya projek akhir ini. Sehingga penulis ingin menyampaikan terimakasih kepada:

1. Allah Subhanahu Wata'ala, atas rahmat dengan segala karunia dan nikmat-Nya, sehingga pembuatan projek akhir ini dapat terselesikan.
2. Kepada kedua orang tua Abi Abdul Jamil, Umi Nafisah, Kakak-kakak terimakasih atas segala dukungan dan doa untuk kelancaran dalam projek akhir ini.
3. Bapak Adi Hermansyah, M.T selaku Dosen Pembimbing I dalam pembuatan Projek Akhir dan rangkaian alat dari awal hingga selesai.
4. Ibu Nurul Afifah, S.Kom, M.Kom selaku Dosen Pembimbing II dalam pembuatan Projek Akhir dan rangkaian alat dari awal hingga selesa.
5. Bapak Adi hermansyah, M.T. selaku Dosen Pembimbing Akademik
6. Bapak Ahmad Heryanto, S.Kom., M.T selaku Koordinator Program Studi Teknik Komputer Universitas Sriwijaya.
7. Bapak dan Ibu Dosen Program Studi Komputer Universitas Srwijaya.
8. Staff di Program Studi Teknik Komputer, khususnya Mbak Faula yang telah membantu penyelesaian proses administrasi.
9. Keluarga Besar Fakultas Ilmu Komputer, bagian akademik, kemahasiswaan, tata

usaha,perlengkapan dan keuangan.

10. Seluruh Pimpinan yang ada di lingkungan Fakultas Ilmu Komputer Universitas Sriwijaya.
11. Seluruh teman satu angkatan 2021, khususnya Teknik Komputer 2021 serta Heru, Bagus, Farhan, Fani, Vivi, Dyah, Syifa, Mawar, dan semuanya. Semoga sukses untuk kita semua.
12. Serta Organisasi di Fakultas Ilmu Komputer Universitas Sriwijaya, BGF (Bujang Gadis Fasilkom). Terima kasih atas kesempatannya dalam menjadi keluarga besar, atas ilmu yang telah diberikan serta wadah berbagi yang hangat.
13. Serta semua pihak yang sangat berperan dan berkontribusi selama penulisan projek akhir ini, yang tidak bisa saya sebutkan satu persatu.

Semoga dengan terselesaikannya projek akhir ini dapat bermanfaat untuk menambah wawasan dan pengetahuan bagi kita semua dalam mempelajari Implementasi *Firewall Tarpit* Pada *Router* Sebagai Perlindungan Terhadap Serangan *Port scanning.*

Dalam penulisan laporan ini, penulis menyadari bahwa masih banyak terdapat kekurangan dan ketidak sempurnaan, oleh karena itu penulis mohon saran dan kritik yang membangun untuk perbaikan laporan projek akhir ini, agar menjadi lebih baik dimasa yang akan datang

Palembang, Juli 2024

Penulis

Achmad hasan

IMPLEMENTASI *FIREWALL TARPIT* PADA *ROUTER* SEBAGAI PERLINDUNGAN TERHADAP SERANGAN *PORT SCANNING*

Oleh

Achmad Hasan
NIM 09030582125004

ABSTRAK

Penelitian ini berfokus pada implementasi *firewall tarpit* pada *Router* sebagai perlindungan terhadap serangan *port scanning*. Serangan *port scanning*, yang digunakan oleh penyerang untuk mengidentifikasi layanan aktif pada suatu jaringan, semakin canggih dan sulit dideteksi. Pendekatan konvensional seperti *firewall stateful* dan *intrusion detection system* memiliki keterbatasan dalam mendeteksi dan menangani serangan *port scanning* dengan cepat dan efektif. Oleh karena itu, diperlukan solusi yang lebih adaptif dan responsif. *Firewall tarpit* adalah salah satu solusi inovatif yang dapat memperlambat serangan dengan mengurung penyerang dalam sesi yang lambat dan mengkonsumsi sumber daya tinggi, sehingga mengurangi kemampuan penyerang untuk melanjutkan serangannya. Penelitian ini menunjukkan bahwa implementasi *firewall tarpit* pada *Router* berhasil melindungi jaringan secara efektif dari serangan *port scanning*. Sistem dapat mengidentifikasi dan memblokir upaya serangan, mencegah akses tidak sah ke dalam jaringan dan perangkat yang ada di dalamnya. Penerapan pada *filtered port services* juga terbukti efektif dalam melindungi *port remote access login* dengan pengaturan yang tepat pada *port* 21, *port* 22, *port* 23, dan *port* 80. Kesimpulannya, *firewall tarpi*t memberikan lapisan keamanan yang lebih efektif pada tingkat *Router*, melindungi seluruh jaringan dari serangan *port scanning* tanpa mengorbankan kinerja jaringan secara signifikan. Untuk penelitian selanjutnya, disarankan untuk mengkombinasikan firewall tarpit dengan metode keamanan jaringan lainnya dan menggunakan alat hacking yang lebih canggih untuk meningkatkan pertahanan jaringan terhadap serangan cyber yang semakin kompleks dan canggih.

Kata Kunci: *firewall tarpit, Router, port scanning,* keamanan jaringan, keamanan informasi.

IMPLEMENTATION OF TARPIT FIREWALL ON ROUTER AS PROTECTION AGAINST *PORT SCANNING* ATTACKS

By

Achmad Hasan

NIM 09030582125004

ABSTRACT

This research focuses on the implementation of a tarpit firewall on Router as protection against *port scanning* attacks. *Port scanning* attacks, used by attackers to identify active services on a network, are becoming increasingly sophisticated and difficult to detect. Conventional approaches, such as stateful firewalls and intrusion detection systems, have limitations in quickly and effectively detecting and handling *port scanning* attacks. Therefore, more adaptive and responsive solutions are required. The tarpit firewall is one innovative solution that can slow down attacks by trapping attackers in slow sessions and consuming high resources, thus reducing the attackers' ability to continue their attacks. This research shows that the implementation of a tarpit firewall on Router effectively protects the network from *port scanning* attacks. The system can identify and block attack attempts, preventing unauthorized access to the network and its devices. The application to filtered *port* services also proved effective in protecting remote access login *port*s with appropriate settings on *port* 21, *port* 22, *port* 23, and *port* 80. In conclusion, the tarpit firewall provides a more effective security layer at the Router level, protecting the entire network from *port scanning* attacks without significantly compromising network performance. For future research, it is recommended to combine the tarpit firewall with other network security methods and use more sophisticated hacking tools to enhance network defense against increasingly complex and sophisticated cyber attacks.

Keywords:tarpit firewall, Router, *port scanning*, network security, information security

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

BAB I PENDAHULUAN

1.1 Latar Belakang

Di era digitalisasi seperti sekarang ini teknologi dan ilmu komunikasi berjalan sangatlah pesat, dimulai dari berkembangnya komputer, *Artificial Intelligence*, *smartphone,* dan jaringan komputer merupakan teknologi informasi yang berkembang sangat pesat saat ini. meningkatnya perkembangan terhadap teknologi informasi dan jaringan, membuat keamanan informasi menjadi suatu hal yang sangat penting.[1]

Pada saat sebuah perangkat terhubung kedalam jaringan *internet* hal pertama yang harus kita perhatikan adalah keamanan jaringan agar data kita aman saat menggunakan *internet.* Dengan perkembangan keamanan jaringan ternyata tidak sepenuhnya menjaga data kita dari seorang *hacker.* Banyak cara yang bisa dilakukan oleh seorang *hacker* untuk bisa mencuri data kita salah satunya adalah dengan cara *port scanning. Port scanning* merupakan teknik yang umum digunakan oleh penyerang untuk mengidentifikasi layanan yang aktif pada suatu jaringan. Serangan terhadap jaringan seperti *port scanning* menjadi lebih canggih dan sering kali sulit dideteksi sehingga serangan *port scanning* dapat membuka peluang bagi serangan selanjutnya seperti *brute force* atau *penetration testing.* Metode konvensional seperti blocking IP yang mencurigakan mungkin tidak lagi cukup efektif, mengingat *fleksibilita*s dan ketidakgunaan serangan *port scanning.*[2]

Pendekatan konvensional dalam mengatasi serangan *port scanning*, seperti menggunakan *firewall stateful* atau *intrusion detection system*, mungkin memiliki keterbatasan dalam mendeteksi dan menangani serangan dengan cepat dan efektif. Maka daripada itu diperlukan solusi yang lebih adaptif dan responsif. Salah satu solusi inovatif yang menarik perhatian dalam melawan serangan *port scanning* adalah penggunaan *firewall tarpit. Firewall tarpit* dapat memperlambat serangan dengan mengurung penyerang dalam sesi yang lambat dan konsumsi sumber daya yang tinggi, sehingga sangat efektif mengurangi kemampuan penyerang untuk

meneruskan serangannya. *Router*, sebagai perangkat networking yang popular dan memiliki kemampuan konfigurasi yang luas, menjadi pilihan tepat untuk dijadikan *platform* implementasi *firewall tarpit.* Penggunaan *firewall* memberikan lapisan keamanan yang lebih efektif pada tingkat Router, sehingga melindungi seluruh jaringan dari serangan *port scanning*.[3]

Memilih solusi keamanan dan keseimbangan antara efektivitas dan kinerja jaringan adalah menjadi sebuah kunci, sehingga *firewall tarpit* diharapkan memberikan perlindungan yang memadai tanpa merugikan kinerja jaringan secara signifikan, sehingga organisasi dapat menjaga keberlanjutan operasional tanpa mengorbankan keamanan. Penelitian ini tidak hanya bertujuan untuk menanggapi ancaman saat ini, tetapi juga untuk mendukung tren keamanan jaringan masa depan. Dengan melibatkan teknologi inovatif seperti *firewall tarpit,* sehingga kita dapat menghadapi tantangan keamanan yang akan terus berkembang.

Berdasarkan uraian di atas, penulis ingin menjadikan masalah ini sebagai fokus penelitian dalam penyusunan Tugas Akhir dengan judul **"IMPLEMENTASI *FIREWALL TARPIT* PADA *ROUTER* SEBAGAI PERLINDUNGAN TERHADAP SERANGAN *PORT SCANNING*"**

1.2 Rumusan Masalah

Berdasarkan identifikasi masalah yang telah disampaikan pada latar belakang,dalam projek ini tersusunlah beberapa rumusan masalah, diantaranya adalah :

1. Bagaimana implementasi *firewall tarpit* untuk mengatasi serangan *port scanning* pada *Router* ?
2. Bagaimana *filtered port service* melindungi *Router* terhadap *port scanning* ?

1.3 Tujuan

Pengimplementasian firewall tarpit pada Router :

1. Melindungi jaringan dari serangan *port scanning*
2. Melakukan *filtered port services* pada *Router*

1.4 Manfaat

Berdasarkan pada tujuan penyusunan projek, terdapat beberapa manfaat yang diberikan, yaitu :

1. Memberikan keamanan jaringan yang efektif dan efisien dari serangan *port scanning*
2. Memberikan perlindungan *port remote access login* pada *Router*

1.5 Batasan Masalah

Adapun Batasan masalah dalam penelitian ini sebagai berikut :

1. Penelitian ini terbatas pada analisis dan perlindungan serangan *port scanning* saja.
2. Penelitian ini lebih berfokus pada penerapan *firewall tarpit* pada skala menengah saja.

1.6 Metode Penelitian

Dalam penyusunan projek ini, beberapa metode yang digunakan antara lain :

1. Metode literature

Metode literatur merupakan cara mendapatkan informasi atau data terkait dengan topik yang dipilih dari berbagai sumber referensi. Sumber-sumber yang digunakan berasal dari website, buku, internet dan artikel jurnal yang sesuai dengan judul **"Implementasi *Firewall Tarpit* Pada *Router* Sebagai Perlindungan Terhadap *Serangan Port scanning*"**

2. Metode Observasi

Dalam projek ini, metode observasi yang digunakan adalah melihat dan mempelajari secara langsung bagaimana *firewall tarpit* dapat digunakan untuk mendeteksi serangan *port scanning*.

3. Metode Konsultasi

Metode konsultasi merupakan salah satu metode yang digunakan dengan cara berdiskusi dengan melakukan tanya jawab bersama dosen pembimbing

untuk dapat menyempurnakan laporan projek baik dalam proses perancangan maupun pembuatan.

4. Metode Implementasi dan pengujian

a. Metode Implementasi

Mengimplementasikan desain dan konfigurasi pada Router serta Menyusun Langkah-langkah implementasi secara rinci, termasuk penggunaan perangkat keras dan perangkat lunak yang diperlukan

b. Metode Pengujian

Melakukan uji coba internal untuk memastikan bahwa *firewall tarpit* berfungsi seperti yang diharapkan, serta memeriksa kemampuan mendeteksi dan memperlambat serangan *port scanning*.

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penyusunan proyek berfungsi untuk mempermudah penulisan penulis. Sistematika penulisan tersebut yaitu :

1. BAB I

   Penulis memberikan penjelasan singkat tentang latar belakang dalam penelitian, rumusan masalah dalam penelitian, dan batasan masalah dalam penelitian, tujuan penelitian, manfaat penelitian, metodologi penelitian.
2. BAB II

   Membahas informasi umum atau teori pendukung yang digunakan sebagai landasan penelitian seperti penelitian terdahulu, serta istilah dan pengertian yang relevan.
3. BAB III

   Bab ini berisi deskripsi sistematis tentang kerangka sistem, topologi jaringan, skenario penelitian , serta konfigurasi atau desain peralatan dan bahan yang akan digunakan.
4. BAB IV

   Bab ini menyajikan uraian tentang hasil implementasi dan sistem kerja *firewall tarpit* pada *Router*.

5. BAB V

   Bab ini menguraikan kesimpulan dari hasil percobaan yang telah dilakukan pada Bab IV, termasuk sejauh mana hasilnya sesuai dengan harapan peneliti. Selain itu, disampaikan pula saran kepada peneliti untuk mempertimbangkan penggunaan *rules action* lainnya dalam penelitian selanjutnya.

DAFTAR PUSTAKA

[1] Muh. S. Alansyar1) and M. C. , Nila Feby Puspitasari, S.Kom, "ANALISA DAN PERANCANGAN KEAMANAN OTENTIKASI VPN SERVER MENGGUNAKAN METODE *PORT* KNOCKING PADA UPT LABORATORIUM UNIVERSITAS AMIKOM YOGYAKARTA," pp. 6–18, 2017.

[2] F. T. Industri and U. I. Indonesia, "MELALUI PENGGUNAAN FIREWALL DENGAN," 2023.

[3] W. Purnama, "ANALISIS DAN PERANCANGAN SISTEM PENGAMANAN AKSES OTENTIKASI MENGGUNAKAN METODE *PORT* KNOCKING DAN FIREWALL ACTION TARPIT PADA MIKROTIK RB951-2n," 2014.

[4] L. Ma and D. Zhao, "Research on Setting of Two Firewall Rules Based on Ubuntu Linux System," *Proceedings - 2022 International Conference on Computer Network, Electronic and Automation, ICCNEA 2022*, pp. 178–182, 2022, doi: 10.1109/ICCNEA57056.2022.00048.

[5] Susanto, A. F. Daru, and F. W. Christanto, "Packet Filtering Gateway and Application Layer Gateway on Mikrotik Router Based Firewalls for Server and Internet Access Restrictions.," in *2023 International Conference on Technology, Engineering, and Computing Applications (ICTECA)*, IEEE, Dec. 2023, pp. 1–6. doi: 10.1109/ICTECA60133.2023.10490754.

[6] P. Anggraeni, A. R. Harits M., and M. Fikri Radhea, "Identifying SCADA Network Security Through Network Reconnaissance and Firewall Filter," in *2021 3rd International Symposium on Material and Electrical Engineering Conference (ISMEE)*, IEEE, Nov. 2021, pp. 211–216. doi: 10.1109/ISMEE54273.2021.9774069.

[7] Y. Katsura, P. Sakarin, N. Yamai, H. Kimiyama, and V. Visoottiviseth, "Quick Blocking Operation of Firewall System Cooperating with IDS and

SDN," in *2022 24th International Conference on Advanced Communication Technology (ICACT)*, IEEE, Feb. 2022, pp. 393–398. doi: 10.23919/ICACT53585.2022.9728831.

[8] E. S. Sagatov, S. Mayhoub, A. M. Sukhov, F. Esposito, and P. Calyam, "Proactive Detection for Countermeasures on *Port scanning* based Attacks," *Proceedings of the 2021 17th International Conference on Network and Service Management: Smart Management for Future Networks and Services, CNSM 2021*, pp. 402–406, 2021, doi: 10.23919/CNSM52442.2021.9615577.

[9] M. Patel, P. P. Amritha, V. B. Sudheer, and M. Sethumadhavan, "DDoS Attack Detection Model using Machine Learning Algorithm in Next Generation Firewall," *Procedia Comput Sci*, vol. 233, pp. 175–183, 2024, doi: 10.1016/j.procs.2024.03.207.

[10] J. Huang, J. Chen, X. Lu, B. Mo, C. Zeng, and S. Qiu, "Research on detection techniques for scanning attacks in software-defined network environments," in *2023 4th International Conference on Computer Engineering and Application, ICCEA 2023*, IEEE, Apr. 2023, pp. 115–118. doi: 10.1109/ICCEA58433.2023.10135250.

[11] F. Yu and X. Chen, "Research on Collaborative Technology of IPv6 Protocol and Firewall Based on IPSec," in *2022 International Conference on Informatics, Networking and Computing (ICINC)*, IEEE, Oct. 2022, pp. 130–133. doi: 10.1109/ICINC58035.2022.00033.

[12] Q. Ismail, O. Saleh, M. Hashayka, A. Awad, A. Hawash, and O. Othman, "Improve the firewall accuracy by using dynamic ontology," *ACM International Conference Proceeding Series*, 2020, doi: 10.1145/3440749.3442607.

[13] G. de Carvalho Bertoli, L. A. Pereira Júnior, and O. Saotome, "Improving detection of scanning attacks on heterogeneous networks with Federated Learning," *ACM SIGMETRICS Performance Evaluation Review*, vol. 49, no. 4, pp. 118–123, Jun. 2022, doi: 10.1145/3543146.3543172.

[14] M. M. Najafabadi, T. M. Khoshgoftaar, C. Calvert, and C. Kemp, "Detection of SSH Brute Force Attacks Using Aggregated Netflow Data," in *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*, IEEE, Dec. 2015, pp. 283–288. doi: 10.1109/ICMLA.2015.20.

[15] R. Albar and R. O. Putra, "Sniffing Dan Implementasi Keamanan Jaringan Network Security Analysis Using the Method Sniffing and Implementation of Network Security on Microtik Router Os V6 . 48 . 3 Using *Port* Knocking Method," *Journal of Informatics and Computer Science*, vol. 8, no. 1, p. 3, 2022.

[16] F. Muhammad, I. Wahidah, and A. I. Irawan, "ANALISIS PENDETEKSIAN SERANGAN DENIAL OF SERVICE (DOS) MENGGUNAKAN LOGIKA FUZZY METODE MAMDANI PADA JARINGAN INTERNET OF THINGS (IOT) DENIAL OF SERVICE (DOS) DETECTION ANALYSIS USING FUZZY LOGIC MAMDANI METHOD ON INTERNET OF THINGS (IOT) NETWORK."

[17] J. D. Santoso, "Analisis Perbandingan Metode Queue Pada Mikrotik," *Pseudocode*, vol. 7, no. 1, pp. 2–3, 2020, doi: 10.33369/pseudocode.7.1.1-7.

[18] G. H. A. Kusuma, "Perancangan Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19," *Journal of Informatics and Advanced …*, vol. 2, no. 2, pp. 1–4, 2021.

[19] Paloaltonetworks.com, "what is a packet filtering firewall", [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-packet-filtering-firewall

[20] Citraweb.com, "Mengelabuhi aplikasi *port scanning* dengan firewal tarpit." Accessed: Mar. 02, 2024. [Online]. Available: https://citraweb.com/artikel

[21] M. R. Dwi Setiawan, Ridwansyah, "Perancangan Keamanan Jaringan Next-Generation Firewall Menggunakan Router Fortinet Pada Pt. Alodokter

Teknologi Solusi," *Jurnal Informatika Terpadu*, vol. 9, no. 1, pp. 34–39, 2023.

[22] F. Ardianto, "PENGGUNAAN MIKROTIK ROUTER SEBAGAI JARINGAN SERVER."

[23] A. P. Martselane Adias Sabara1, "Konfigurasi Menejemen Bandwidth Menggunakan Router Mikrotik RB2011UiAS-RM," *Jurnal Power Elektronik*, vol. 9, no. 2, p. 44, 2020.

[24] S. Dwiyatno, "Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap," *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, vol. 7, no. 2, p. 111, 2020, doi: 10.30656/prosisko.v7i2.2522.

[25] A. Fauzi, "Implementasi Load Balancing Peer Connection Classifier (pcc) Pada Jaringan Internet Di Rumah Sakit Umum Daerah Prabumulih"," *Univ Bina Darma*, pp. 1–10, 2020.

[26] M. A. Sabara, A. M. Harimadi, and I. Safii, "Rancang Bangun Dns Server Berbasis Linux Ubuntu Di Pt.Graha Service Indonesia Sebagai Media Pengolahan Jaringan Internet," *Jurnal POLEKTRO: Jurnal Power Elektronik*, vol. 8, no. 2, 2020.

[27] N. F. Zamzami, "Ismplementasi load balancing dan failover menggunakan mikrotik router os berdasarkan multihomed gateway pada warung internet "diga"," *Implementasi load balancing dan failover menggunakan mikrotik router os berdasarkan multihomed gateway pada warung internet "diga"*, p. 12, 2005.

[28] S. Dwiyatno, E. Rachmat, A. P. Sari, and O. Gustiawan, "Implementasi Virtualisasi Server Berbasis Docker Container," *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, vol. 7, no. 2, pp. 165–175, 2020, doi: 10.30656/prosisko.v7i2.2520.