Research Article
FORBIS: Forensics Business Information System Journal
Published online on: https://journal.universitasmulia.ac.id/index.php/forbis **1 (2) Agustus 2024**

PERANCANGAN DAN IMPLEMENTASI KEAMANAN DAN PENGEMBANGAN INFRASTRUKTUR JARINGAN (Studi Kasus: CV. Klix Refill Center Balikpapan)

Ade Kamal[1], Richki Hardi[2], Nasruddin Bin Idris[3]*

[1,2,3]Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Mulia

email: [1]adekamal@students.universitasmulia.ac.id, [2]richki@universitasmulia.ac.id, [3]nasruddin@universitasmulia.ac.id
[*]Correspondence

ARTICLE INFO

Article History
Received : 6 June 2023
Revised : 13 Agustus 2024
Accepted : 18 Agustus 2024
Available online : 18 Agustus 2024

Keywords:
Network Security, Network Infrastructure, Login Hotspot, MAC Address Filtering, Mikrotik

ABSTRACK

In the rapidly developing digital era, security and efficiency in network management are top priorities. This study aims to design and implement a secure and integrated network system at CV. Klix Refill Center Balikpapan. Through this design, research offers security solutions and network infrastructure development. The login hotspot configuration is used to provide logged access to the network, ensuring that only authorized users can connect. To further enhance security, MAC address filtering is implemented, enabling tighter access control and preventing unauthorized access. Subnetting is implemented to optimize the use of IP addresses. In addition, Telegram bots are integrated to monitor login and logout activities of hotspot users in real-time. The results of this study indicate that the combination of login hotspot configuration, MAC address filtering, subnetting, and monitoring with Telegram bots is expected to create a more secure, quiet, and responsive network infrastructure.

ABSTRAK

Dalam era digital yang berkembang pesat, keamanan dan efisiensi dalam manajemen jaringan menjadi prioritas utama. Studi ini bertujuan untuk merancang dan mengimplementasikan sistem jaringan yang aman dan terintegrasi pada CV. Klix Refill Center Balikpapan. Melalui perancangan ini, penelitian menawarkan solusi keamanan dan pengembangan infrastruktur jaringan. Konfigurasi hotspot login digunakan untuk memberikan akses terkontrol ke jaringan, memastikan bahwa hanya pengguna yang sah yang dapat terhubung. Untuk meningkatkan keamanan lebih lanjut, filtering MAC address diimplementasikan, memungkinkan kontrol akses yang lebih ketat dan mencegah akses yang tidak sah. Subnetting diterapkan untuk mengoptimalkan penggunaan alamat IP. Sebagai tambahan bot Telegram diintegrasikan untuk memantau aktivitas login dan logout pengguna hotspot secara real-time. Hasil penelitian ini menunjukkan bahwa kombinasi dari konfigurasi hotspot login, filtering MAC address, subnetting, dan monitoring dengan bot

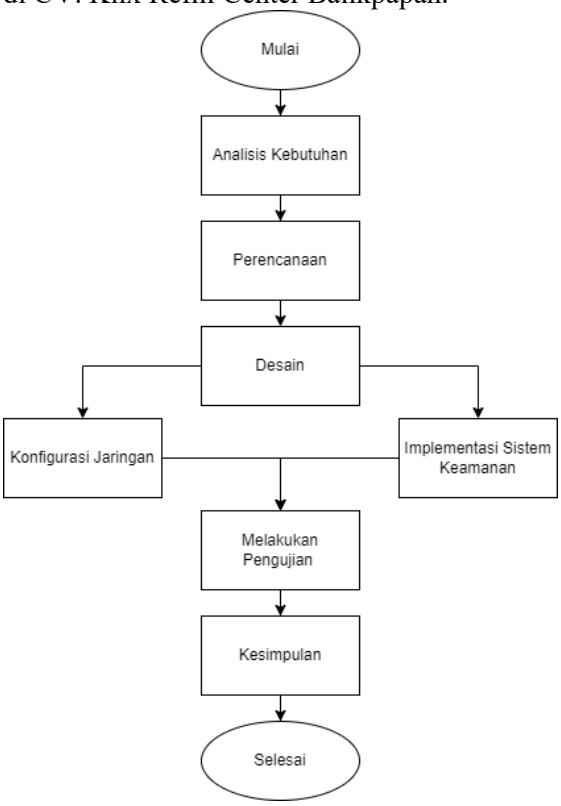
Telegram diharapkan menciptakan infrastruktur jaringan yang lebih aman, terkontrol, dan responsif.

1. Pendahuluan

Perkembangan teknologi informasi yang pesat di era digital saat ini tidak hanya membawa manfaat, namun juga ancaman bagi setiap perusahaan. Khususnya adalah CV. Klix Refill Center, sebuah perusahaan yang beroperasi di sektor layanan perbaikan dan penjualan printer di Balikpapan. Keamanan dan infrastruktur jaringan juga dibutuhkan untuk membantu dalam berbagai operasional di perusahaan maupun CV. Klix Refill Center. CV. Klix Refill Center memanfaatkan jaringan nirkabel. Penyebaran jaringan dilakukan hanya menggunakan modem ISP untuk menghubungkan lima perangkat komputer yang tersedia. CV. Klix Refill Center mengandalkan SSID dan kata sandi untuk keamanan jaringannya. Dengan hanya menggunakan kata sandi, pengguna dapat terhubung ke dalam jaringan perusahaan. Namun model keamanan jaringan seperti ini sangat rentan dari serangan serta kejahatan oleh pihak yang tidak bertanggung jawab. Permasalahan yang dihadapi CV. Klix Refill Center Balikpapan adalah menjaga keamanan jaringan nirkabel mereka dari pengguna tidak berizin yang tidak dikenali menggunakan akses jaringan. Sebagai solusi, untuk mengimplementasikan keamanan jaringan ini diperlukan sejumlah perangkat yang dapat memenuhi fitur keamanan yang dibutuhkan. Contoh perangkat tersebut adalah perangkat keras seperti mikrotik untuk merancang konfigurasi jaringan hotspot login dengan keamanan username dan kata sandi, filtering MAC address, menerapkan subnetting dan menerapkan monitoring pada user hotspot yang login dan logout dengan aplikasi telegram. Dengan ini penulis tertarik untuk membuat judul “Perancangan dan Implementasi Keamanan dan Pengembangan Infrastruktur Jaringan di CV. Klix Refill Center Balikpapan.

2. Metode Penelitian

Untuk metode penelitian ini yang berjudul "Perancangan dan Implementasi Keamanan dan Pengembangan Infrastruktur Jaringan (Studi Kasus: CV. Klix Refill Center Balikpapan) penulis akan menggunakan metode penelitian Network Development Life Cycle (NDLC).
NDLC ini sebuah kerangka kerja yang digunakan untuk merencanakan, menerapkan, mengelola jaringan komputer beserta keamanan dan infrastruktur perangkat jaringan di CV. Klix Refill Center Balikpapan.



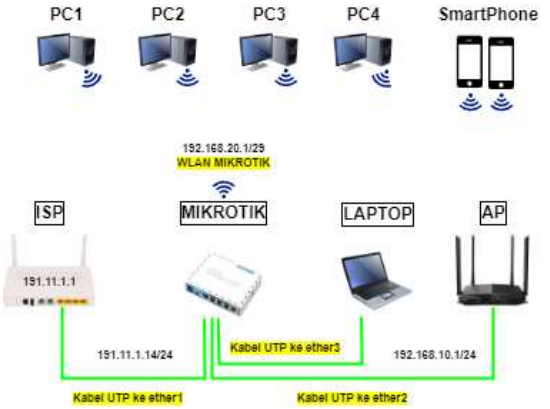
Gambar 1. Alur Penelitian

Merujuk pada gambar 1 merupakan flowchart metode penelitian yang akan dilakukan.

3. Hasil dan Pembahasan

Pada tahap gambaran perancangan ini terdapat beberapa perangkat seperti modem ISP, mikrotik, laptop, access point, komputer ,

dan smartphone. Pada modem ISP akan dihubungkan dengan kabel UTP ke ether1 mikrotik, laptop akan dihubungkan ke ether3 mikrotik untuk melakukan konfigurasi jaringan dan sistem keamanannya, access point akan dihubungkan ke ether2 mikrotik untuk membagikan jaringan secara nirkabel ke smartphone, dan pada wlan internal mikrotik akan digunakan sebagai access point bridge dengan fitur hotspot untuk empat komputer yang tersedia. Berikut merupakan gambaran perancangan yang akan dikonfigurasi pada Gambar 6 dibawah ini.

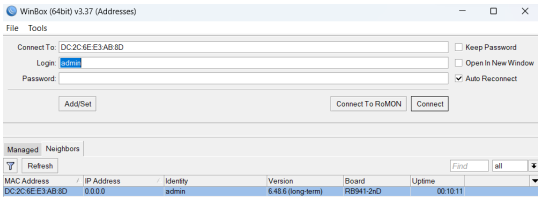


Gambar 2. Gambaran Perancangan

A. Konfigurasi jaringan.

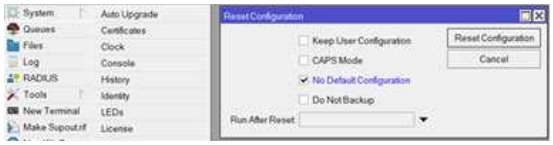
Pada tahap ini akan membuat konfigurasi jaringan berupa hotspot di perangkat lunak winbox. Perangkat lunak winbox ini disediakan oleh mikrotik untuk memudahkan proses konfigurasi. Berikut tahapan dari konfigurasinnya:

1. Buka perangkat lunak winbox seperti pada Gambar 3 berikut.



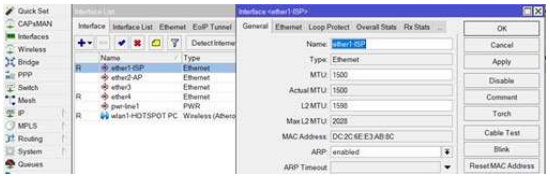
Gambar 3. Tampilan Login Winbox

2. Reset konfigurasi default seperti pada Gambar 4 berikut.



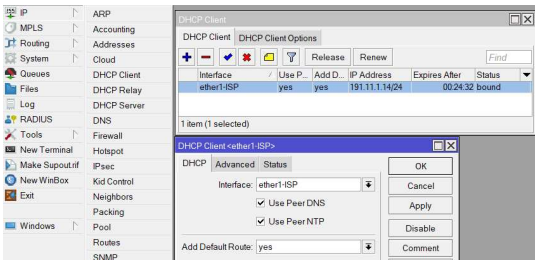
Gambar 4. Reset Kofigurasi Default

3. Memberikan nama setiap interface.



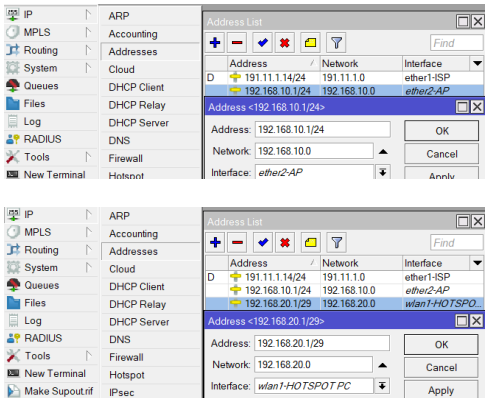
Gambar 5. Interface List

4. Buat DHCP Client.



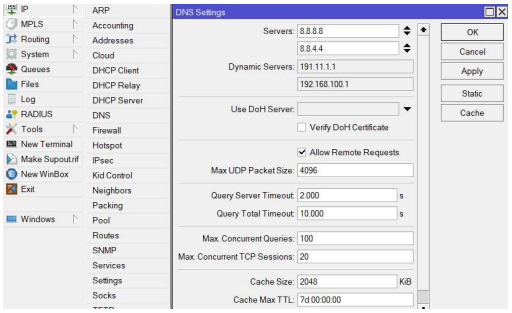
Gambar 6. DHCP Client

5. Memberikan IP ether2 dan wlan1.



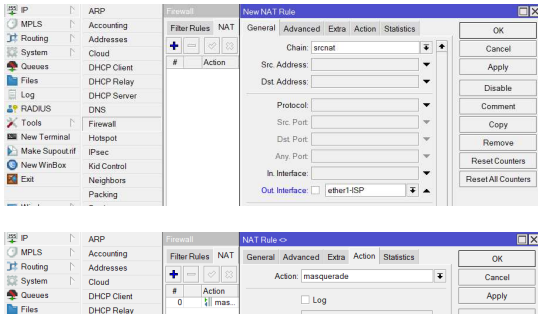
Gambar 7. IP ether2 dan wlan1

6. Setting DNS.



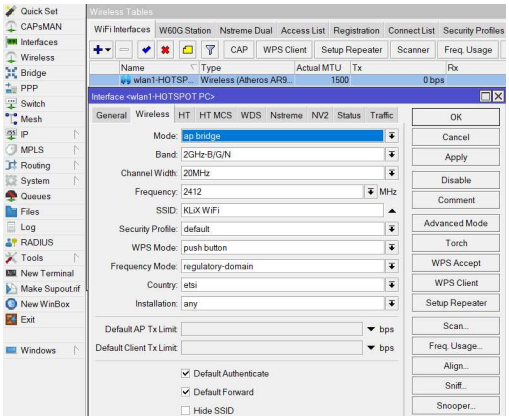
Gambar 8. DNS

7. Setting Firewall NAT.



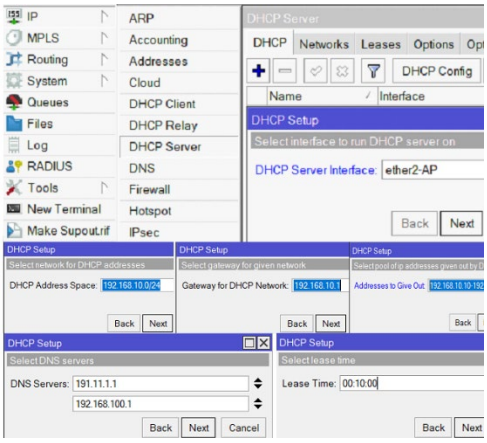
Gambar 13 Firewall NAT

8. Setting wireless interface ke AP bridge.



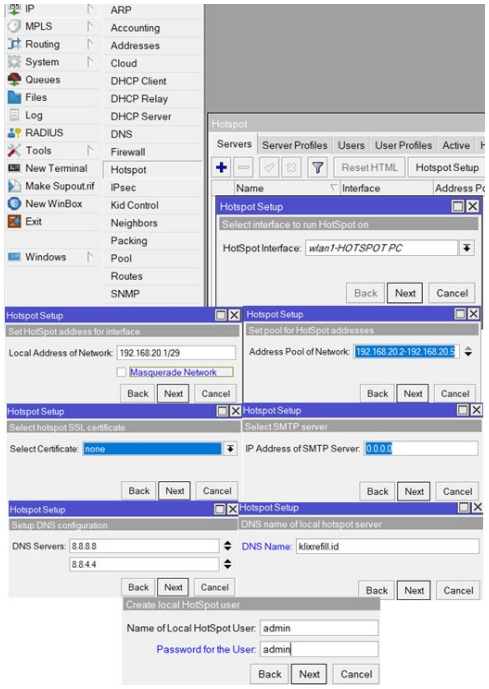
Gambar 14 Wireless Interface AP bridge

9. Buat DHCP server ether2.



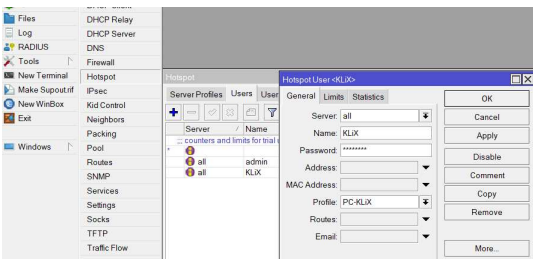
Gambar 15 DHCP server ether2

10. Buat hotspot setup.



Gambar 16 Hotspot Setup

11. Buat user hotspot.

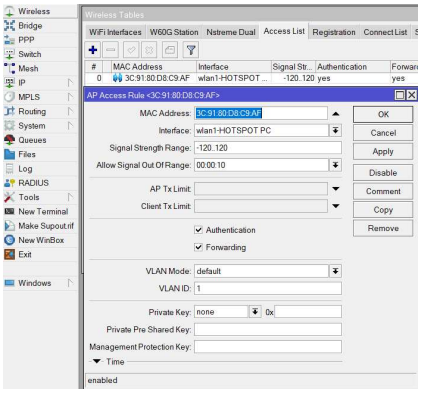


Gambar 17 User Hotspot

B. Implementasi sistem keamanan

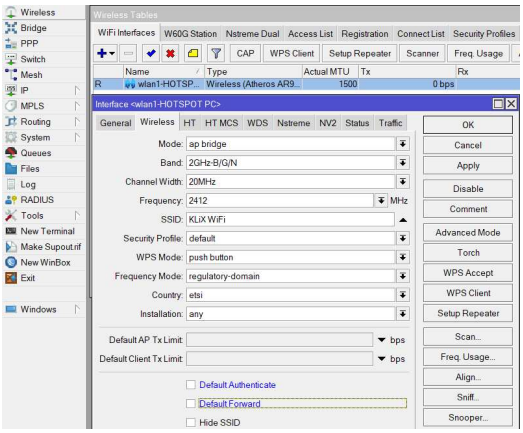
Sistem keamanan filtering MAC address.

1. Daftarkan MAC address perangkat yang dibutuhkan.



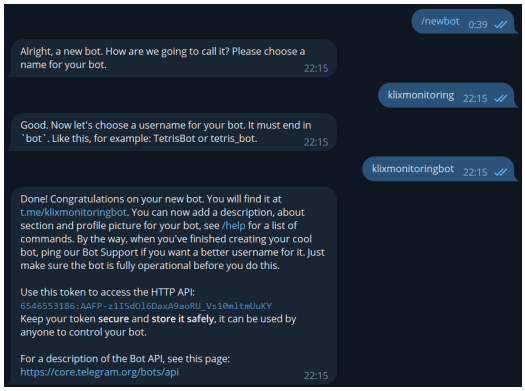
Gambar 18 Daftarkan MAC address perangkat

2. Non aktifkan default authenticate dan default forward pada interface wlan1.



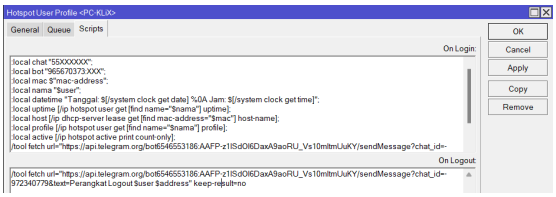
Gambar 19 Default Authenticate dan Default Forward

3. Monitoring hotspot user login dan logout dengan bot telegram.



Gambar 20 Bot Telegram

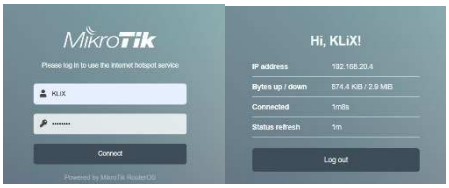
4. Script login dan logout bot telegram di winbox.



Gambar 21 Script Login dan Logout

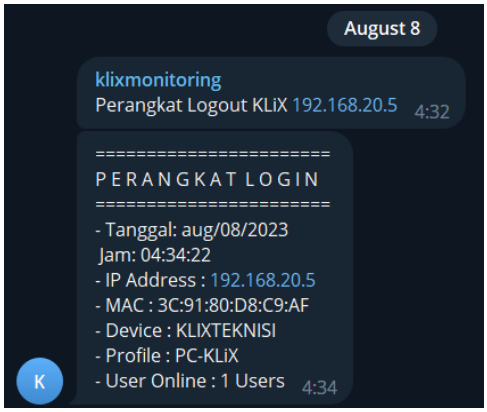
C. Pengujian

1. Hasil konfigurasi hotspot login username dan password.



Gambar 22 Pengujian Login Hotspot

2. Pengujian monitoring hotspot user login dan logout di bot telegram.



Gambar 23 Pengujian Monitoring Hotspot

4. Kesimpulan

Dari penelitian yang telah dilaksanakan, dapat ditarik kesimpulan bawah Peningkatan infrastruktur jaringan dengan melalui penambahan perangkat Mikrotik dan access point, infrastruktur jaringan di CV. Klix Refill Center Balikpapan dapat dikembangkan dengan perancangan jaringan hotspot dan sistem keamanan yang diterapkan, konfigurasi hotspot login mikrotik membantu dalam autentikasi pengguna dari perangkat komputer, sehingga hanya pengguna yang berwenang yang dapat mengakses jaringan, implementasi sistem keamanan filtering MAC address dapat meningkatkan keamanan jaringan dengan membatasi akses hanya untuk alamat MAC yang terdaftar dari perangkat komputer, sehingga mengurangi risiko akses yang tidak sah, monitoring melalui bot telegram dapat memantau login dan logout pengguna membantu dalam pemantauan real-time terhadap aktivitas dalam jaringan. Hal ini memungkinkan respon yang cepat terhadap aktivitas yang mencurigakan.

Referensi

[1] J. E. W. Prakasa, "Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi," *Jurnal Ilmiah Teknologi Informasi Asia*, vol. 14, no. 2, p. 75, May 2020, doi: 10.32815/jitika.v14i2.452.

[2] A. Wijayanto, I. Riadi, and Y. Prayudi, "TAARA Method for Processing on the Network Forensics in the Event of an ARP Spoofing Attack," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, no. 2, pp. 208–217, Mar. 2023, doi: 10.29207/resti.v7i2.4589.

[3] A. Wijayanto, I. Riadi, Y. Prayudi, and T. Sudinugraha, "Network Forensics Against Address Resolution Protocol Spoofing Attacks Using Trigger, Acquire, Analysis, Report, Action Method," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 8, no. 2, pp. 156–169, Jul. 2022, doi: 10.26594/register.v8i2.2953.

[4] M. Muqorobin, Z. Hisyam, M. Mashuri, H. Hanafi, and Y. Setiyantara, "Implementasi Network Intrusion Detection System (NIDS) Dalam Sistem Keamanan Open Cloud Computing," *Majalah Ilmiah Bahari Jogja*, vol. 17, no. 2, pp. 1–9, Jul. 2019, doi: 10.33489/mibj.v17i2.205.

[5] E. Stephani, Fitri Nova, and Ervan Asri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 1, no. 2, pp. 67–74, Dec. 2020, doi: 10.30630/jitsi.1.2.10.

[6] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 4, no. 2, p. 413, Apr. 2020, doi: 10.30865/mib.v4i2.2037.

[7] T. Widodo and A. S. Aji, "Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS)," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 7, no. 1, pp. 46–55, Jan. 2022, doi: 10.14421/jiska.2022.7.1.46-55.

[8] Y. Arta, "Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal," *IT JOURNAL RESEARCH AND DEVELOPMENT*, vol. 2, no. 1, pp. 43–50, Nov. 2017, doi: 10.25299/itjrd.2017.vol2(1).979.

[9] E. Risyad, M. Data, and E. S. Pramukantoro, "Perbandingan Performa Intrusion Detection System (IDS) Snort Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flood," 2018. [Online]. Available: http://j-ptiik.ub.ac.id

[10] L. Lukman and M. Suci, "Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache," *Respati*, vol. 15, no. 2, p. 6, Jul. 2020, doi: 10.35842/jtir.v15i2.343.

[11] Z. A. Tyas, A. Firdonsyah, and W. Ramdhani, "Analisis Keamanan Jaringan dari Serangan DoS pada Sistem Inventaris Sanggar Tari Natya Lakshita menggunakan IDS," *INFORMAL: Informatics Journal*, vol. 7, no. 3, p. 258, Dec. 2022, doi: 10.19184/isj.v7i3.34943.

[8] Tulloh, D. M., Duskarnaen, M. F., & Ajie, H. (2020). Analisis Jaringan Akses Internet Menggunakan Mikrotik Router OS di SMK Tunas Harapan dengan Optimalisasi Load Balancing Menggunakan Parameter QoS (Quality of Service). Jurnal Pinter, 4(1), 1-12.

[9] Saragi, D. R., Sumarno, Nasution, Z. M., Parlina, I., & Anggraini, F. (2021). Implementasi Konfigurasi Hotspot Server Untuk Akses Internet Menggunakan Mikrotik Router Pada Dinas Lingkungan Hidup Pematangsiantar. Jurnal Device, 11(2), 13-20.

[10] Susianto, D. (2016). Implementasi Queue Tree Untuk Manajement Bandwidth Menggunakan Router Board Mikrotik. Jurnal Cendikia, 12(1), 1-10.

[11] Hakim, D. K., & Nugroho, S. A. (2019). Implementasi Telegram Bot untuk Monitoring Mikrotik Router. Sainteks, 16(2), 1-10.

[12] Haryadi, E., Abdussomad, & Robi. (2019). Implementasi Sistem Backup Data Perusahaan Sebagai Bagian dari Disaster Recovery. Sainstech, 29(2), 1-10.

[13] Firmansyah, Purnama, R. A., & Astuti, R. D. (2021). Optimalisasi Keamanan Wireless Menggunakan Filtering MAC Address. Jurnal Teknologi Informasi, 15(1), 1-10.

[14] Sofana, I. (2015). Membangun Jaringan Komputer. Informatika Bandung.

[15] , K. M., & Hendrian, Y. (2016). Analisis Wireless Local Area Network (WLAN) dan Perancangan MAC Address Filtering Menggunakan Mikrotik (Studi Kasus Pada PT. Graha Prima Swara Jakarta). Jurnal Teknik Komputer AMIK BSI, 2(2), 1-10.

[16] Bayunda, N. (2021). Perancangan Sistem Keamanan Jaringan Wireless Local Area Network Pada Kantor Dinas Ketahanan Pangan Kabupaten Bengkalis (Unpublished bachelor's thesis). Universitas Islam Riau, Pekanbaru.

[17] , R. A. (2019). Optimalisasi Keamanan Jaringan Wireless Menggunakan Firewall Filtering MAC Address. Indonesian Journal on Networking and Security, 8(4), 1-10.

[18] Dasmen, R. N., Syarif, A. R., Saputra, H., & Amrullah, R. (2022). Perancangan Keamanan Internet Jaringan Hotspot Mikrotik pada Winbox dan Wireshark. Journal of Computer and Information Technology, 5(2), 71-79.

[19] Kurniawan, R. (2016). Analisis Dan Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode NDLC (Network Development Life Cycle) Pada Bpu Bagas Raya Lubuklinggau. Jurnal Ilmiah Betrik, 7(1), 1-10.