Neptunus: Jurnal Ilmu Komputer Dan Teknologi Informasi
Vol. 2, No. 3 Agustus 2024
e-ISSN: 3031-898X; p-ISSN: 3031-8998, Hal. 16-24
DOI: https://doi.org/10.61132/neptunus.v2i3.177

Analisis Keamanan Jaringan Menggunakan Mikrotik Pada Lab Komputer STMIK Widuri

Seprianus Kenat
Sekolah Tinggi Manejenen Informatika & Komputer Jakarta Selatan, Indonesia
E-mail: kenatseprianus@gmail.com

Abstract: This study discusses the network security analysis using MikroTik devices in the computer laboratory of STMIK Widuri. The main objective of this research is to evaluate the level of network security in the computer laboratory by implementing appropriate configurations using MikroTik devices. The methods employed include literature review on network security, analysis of network topology in the laboratory, and implementation of security solutions using MikroTik devices. Data collected include security testing results, network performance, and user satisfaction levels. The research findings indicate that the implementation of security solutions with MikroTik effectively enhances network security in the computer laboratory of STMIK Widuri. This study contributes to a practical understanding of using MikroTik in improving network security in campus environments.

Keywords: Network Security, Mikrotik, VPN.

Abstrak: Penelitian ini membahas analisis keamanan jaringan menggunakan perangkat MikroTik di laboratorium komputer STMIK Widuri. Tujuan utama penelitian ini adalah untuk mengevaluasi tingkat keamanan jaringan di laboratorium komputer tersebut dengan menerapkan konfigurasi yang sesuai menggunakan perangkat MikroTik. Metode yang digunakan meliputi studi literatur tentang keamanan jaringan, analisis topologi jaringan di laboratorium, dan implementasi solusi keamanan menggunakan perangkat MikroTik. Data yang dikumpulkan mencakup hasil pengujian keamanan, performa jaringan, dan tingkat kepuasan pengguna. Hasil penelitian menunjukkan bahwa penerapan solusi keamanan dengan MikroTik efektif meningkatkan keamanan jaringan di laboratorium komputer STMIK Widuri. Penelitian ini memberikan kontribusi dalam pemahaman praktis tentang penggunaan MikroTik dalam meningkatkan keamanan jaringan di lingkungan Kampus.

Kata kunci: Keamanan jaringan, MikroTik, VPN.

LATAR BELAKANG

Mengingat pesatnya perkembangan teknologi informasi, penggunaan jaringan dalam bisnis dan pendidikan menjadi semakin penting. Namun kenyataannya, jaringan rentan terhadap serangan peretasan dan aktivitas kriminal di dunia maya. Keamanan jaringan sangat penting. Salah satu caranya adalah menerapkan teknik keamanan port-cropping di router untuk meningkatkan keamanan jaringan(Rahman et al., 2020).

Dengan pesatnya perkembangan teknologi saat ini tidak dapat dipungkiri akan adanya dampak serangan terhadap jaringan pada sistem administrator. Sehingga bagi para pengguna teknologi yang terhubung pada jaringan local maupun internet perlu waspada terhadap serangan yang dilakukan oleh pihak yang tidak bertanggung jawab(Manado et al., 2019).

Berdasarkan penelitian ini, ditemukan beberapa masalah yang sering terjadi dalam laboratorium komputer STMIK Widuri, yaitu banyak port yang terbuka seperti port 53/tcp, port 443/tcp, port 1723/tcp, port 2000/tcp. berikut adalah contoh perintah yang dapat digunakan dengan Nmap untuk menganalisis port yang terbuka dihost STMIK Widuri: nmap

Received: Maret 30, 2023; Accepted: Juni 25, 2023; Published: Agustus 31, 2024
* Seprianus Kenat, kenatseprianus@gmail.com

<target>. Untuk menganalisis port yang terbuka di host dengan alamat IP 172.10.11.1:8999, perintahnya akan menjadi nmap 172.10.11.1:8999 Setelah perintah dieksekusi, Nmap akan memulai pemindaian dan memberikan laporan hasilnya. Laporan tersebut akan mencakup daftar port yang terbuka, status port (terbuka atau tertutup), dan layanan yang berjalan di port tersebut.Tujuan dari penelitian ini adalah untuk meningkatkan sistem keamanan dengan lebih baik di masa depan, khususnya dalam lingkungan Laboratorium Komputer STMIK Widuri.

Keamanan jaringan adalah sesuatu yang perlu diingat, Tidak ada jaringan yang memberikan perlindungan terhadap penyadapan, dan tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah untuk berkomunikasi. Komunikasi apa pun bisa jatuh ke tangan yang salah. Sistem keamanan melindungi jaringan tanpa memengaruhi penggunaan jaringan dan secara andal mencegah intrusi jaringan. Mereka yang tidak mengerti ini harus membuat lubang keamanan di jaringan mereka yang sudah ada. Dua faktor utama membentuk keamanan jaringan, Salah satunya adalah tembok keamanan fisik dan virtual yang dipasang antara perangkat dan layanan jaringan yang digunakan dan para penjahat(Desmira & Wiryadinata, 2022).

Keamanan port knocking pada router Mikrotik Router OS dapat dilakukan dengan menggunakan script yang dibuat khusus. Script ini akan melakukan konfigurasi otomatis pada router dan mengaktifkan port knocking(Mulyanto et al., 2021).

Port komunikasi adalah port yang masuk dan keluar dikendalikan di dalam firewall. Port non-esensial dapat diblokir (ditutup), tetapi port kritis dan berbahaya juga dapat diblokir. Misalnya, sambungkan ke internet saat port SSH blokir di server dan akses server web melalui SSH untuk memperbaiki konfigurasi. Koneksi ke Internet terhalang oleh firewall, yang tentunya sangat mengganggu(Amien, 2020).

KAJIAN TEORITIS

1. Pengertian Jaringan Komputer

   Jaringan komputer adalah sebuah sistem yang terdiri dari dua atau lebih komputer yang saling terhubung satu sama lain melalui media komunikasi untuk berbagi data, informasi, dan sumber daya. Jaringan ini dapat berupa jaringan lokal (LAN) atau jaringan yang lebih luas (WAN).

2. Keamanan Jaringan

   Keamanan jaringan adalah tindakan dan kebijakan yang diterapkan untuk melindungi integritas, kerahasiaan, dan ketersediaan data dan sumber daya jaringan. Aspek-aspek penting dalam keamanan jaringan meliputi:

- Kerahasiaan (Confidentiality): Menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang.
- Integritas (Integrity): Menjaga keakuratan dan keutuhan data dari ancaman perusakan.
- Ketersediaan (Availability): Memastikan bahwa data dan sumber daya jaringan tersedia untuk pengguna yang berwenang saat dibutuhkan.

3. MikroTik

MikroTik adalah perusahaan yang dikenal luas karena perangkat keras dan perangkat lunak router yang mereka kembangkan. RouterOS adalah sistem operasi yang dikembangkan oleh MikroTik, yang menyediakan berbagai fitur untuk mengelola jaringan, seperti routing, firewall, bandwidth management, dan VPN.

4. Port knocking

Port Knocking adalah port yang masuk dan keluar dikendalikan di dalam firewall. Port non-esensial dapat diblokir (ditutup), tetapi port kritis dan berbahaya juga dapat diblokir. Misalnya, sambungkan ke internet saat port SSH blokir di server dan akses server web melalui SSH untuk memperbaiki konfigurasi. Koneksi ke Internet terhalang oleh firewall, yang tentunya sangat mengganggu(Amien, 2020).

METODE PENELITIAN

Metode penelitian tentang Analisa Keamanan Jaringan Menggunakan Mikrotik Pada lab Komputer STMIK Widuri adalah suatu penelitian untuk meningkatkan keamanan jaringan dengan menganalisa teknik "knocking" pada Mikrotik Router.

Metode penelitian ini terdiri dari beberapa langkah, diantaranya adalah:

1. Analisa keamanan jaringan

Pada langkah pertama ini dilakukan analisis kebutuhan, analisis permasalahan yang dihadapi, analisis kebutuhan pengguna, dan analisis topologi jaringan yang ada. Metode yang digunakan adalah:

a) Wawancara dilakukan dengan karyawan Puskom tentang manajemen jaringan saat ini dan harapannya.
b) Observasi: Observasi langsung di ruang komputer STMIK Widuri untuk mendapatkan hasil yang lebih efektif, kemudian penjelasan dasar untuk masuk ke tahap desain.

2. Literatur Review

Teknik literatur review yakni sebuah teknik pengumpulan data serta informasi yang berupa: jurnal ilmiah dan buku serta lainnya yang berhubungan dengan topik yang akan diteliti oleh penulis dalam penelitian ini.

HASIL DAN PEMBAHASAN

1. Konfigurasi Mikrotik

1. Masuk ke MikroTik RouterOS melalui antarmuka melalui Winbox.
2. Buka menu "IP" dan pilih "Firewall" untuk mengakses pengaturan firewall.

   Di jendela "Firewall", kita dapat melihat beberapa tab dan opsi konfigurasi yang berbeda:

   a) Filter Rules Tab ini digunakan untuk mengatur aturan firewall untuk memfilter lalu lintas jaringan berdasarkan kriteria tertentu, seperti alamat sumber, alamat tujuan, protokol, dan port. dapat menambahkan, mengubah, atau menghapus aturan firewall di sini.

   b) NAT Tab ini digunakan untuk mengonfigurasi aturan Network Address Translation (NAT), yang berguna untuk mengalihkan lalu lintas jaringan antara alamat IP publik dan alamat IP lokal di jaringan Anda.

   c) Mangle Tab ini digunakan untuk mengkonfigurasi aturan mangle yang memungkinkan Anda mengubah dan mengatur properti paket seperti TOS (Type of Service), TTL (Time to Live),.

   d) Layer7 Protocols Tab ini digunakan untuk mengatur protokol Layer 7 yang memungkinkan mengidentifikasi dan memblokir lalu lintas berdasarkan jenis aplikasi atau protokol tingkat aplikasi.

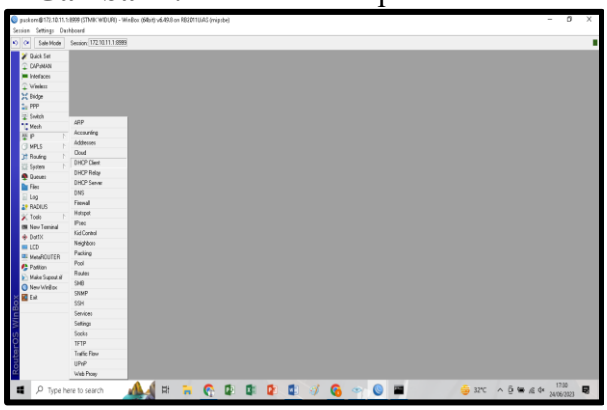
   e) Connection Tracking Tab ini menyediakan informasi tentang koneksi jaringan yang sedang aktif dan memungkinkan Anda mengatur pengaturan pelacakan koneksi.

   f) Service Ports Tab ini digunakan untuk mengatur pengaturan port layanan yang diidentifikasi oleh MikroTik secara otomatis.

   g) Setelah Anda melakukan perubahan pada pengaturan firewall, jangan lupa untuk menyimpan konfigurasi dengan mengklik tombol "Apply" atau "OK" untuk menerapkan perubahan.

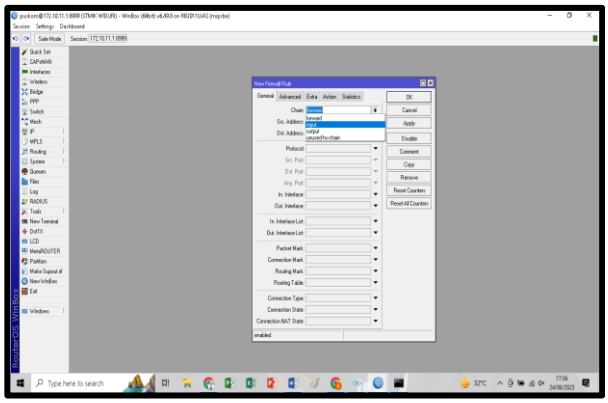
3. Pada tab "Filter Rules", klik tombol "Add New" untuk membuat aturan baru.
4. Pada kolom "Chain", pilih "input" jika ingin menerapkan aturan ini untuk lalu lintas yang masuk ke router.

Gambar 1. Membuat rule pada mikrotik



Sumber Widuri 2024

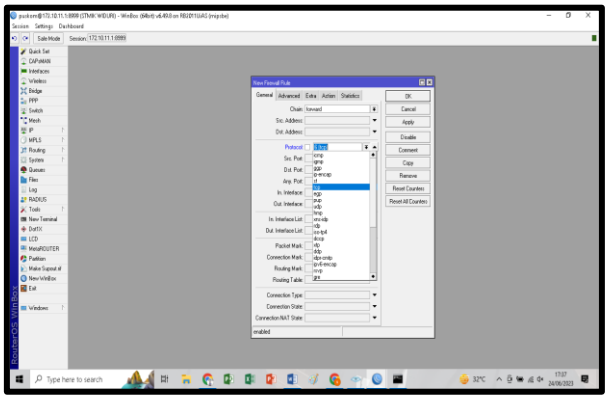
Gambar 2. Membuat Filter



Sumber Widuri 2024

5. Pada kolom "Protocol", pilih protokol yang ingin diterapkan, misalnya "TCP" atau "UDP".

Gambar 3. Pilih Protokol



Sumber widuri 2023

6. Pada kolom "Protocol" dalam konteks konfigurasi port, dapat memilih protokol yang ingin diterapkan. Pilihan yang umum adalah "TCP" (Transmission Control Protocol) atau "UDP" (User Datagram Protocol). Berikut adalah penjelasan singkat tentang kedua protokol ini:
   a. TCP (Transmission Control Protocol) adalah protokol yang handal dan terurutkan dalam pengiriman data. Digunakan untuk aplikasi yang membutuhkan pengiriman data yang andal dan terjamin, seperti transfer file, akses web melalui HTTP, email melalui SMTP dan IMAP, dan sebagainya.
   b. UDP (User Datagram Protocol) adalah protokol yang tidak handal dan tidak terurutkan dalam pengiriman data. Digunakan untuk aplikasi yang lebih ringan dan tidak membutuhkan mekanisme terjamin dalam pengiriman data, seperti layanan streaming, videoconferencing, DNS (Domain Name System), dan lain-lain.

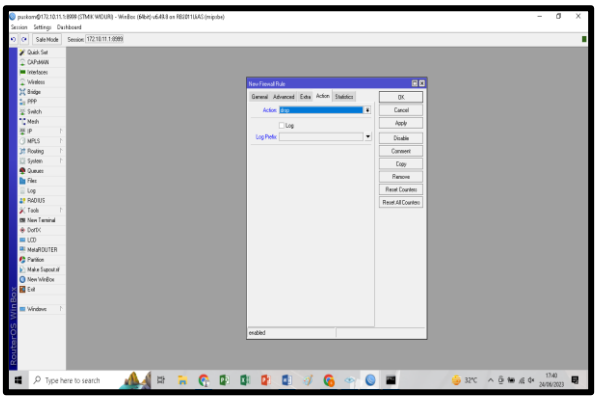
   Dalam konfigurasi port, dapat memilih protokol yang sesuai dengan layanan atau aplikasi yang diinginkan. Misalnya, jika ingin membuka port untuk server web (HTTP), akan memilih protokol "TCP" karena HTTP menggunakan TCP sebagai protokol

transportasinya. Namun, jika ingin membuka port untuk layanan DNS, akan memilih protokol "UDP" karena DNS menggunakan UDP

7. Pada kolom "Dst. Port", masukkan nomor port yang ingin lindungi dari akses komputer yang tidak dikenali. Pada kolom "Action", pilih "Drop" untuk menolak lalu lintas yang mencoba mengakses port tersebut.

Proses ini disebut sebagai konfigurasi firewall untuk melindungi port tertentu dari akses yang tidak diizinkan. Dengan mengatur firewall seperti ini, komputer akan menjadi lebih aman dari serangan jaringan yang berpotensi membahayakan data dan informasi yang tersimpan di dalamnya. Pastikan untuk selalu memperbarui dan memantau pengaturan firewall Anda secara berkala untuk memastikan tingkat keamanan yang optimal, seperti pada gambar dibawah ini.

Gambar 4. Dst Port

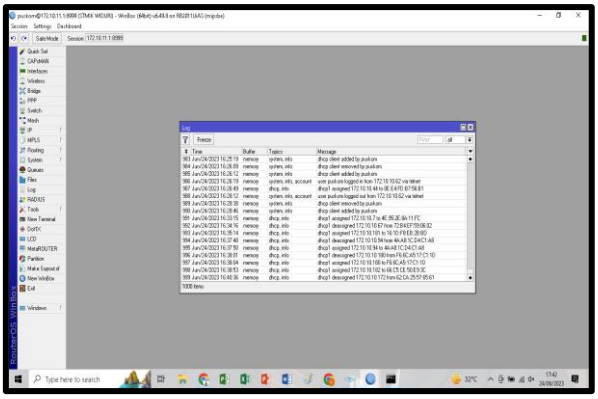


Sumber widuri 2023

8. Klik tombol"OK" untuk menyimpan konfigurasi.

Untuk memastikan bahwa aturan berfungsi dengan baik, perlu memantau log pada MikroTik RouterOS untuk melihat apakah ada aktivitas yang mencoba melanggar aturan tersebut. Buka menu "Sistem" dan pilih "Log" untuk melihat log sistem. dapat memfilter log berdasarkan kategori firewall untuk melihat aktivitas yang terkait dengan aturan firewall yang dibuat. Gambar dibawah ini menunujkan bahwa rule yang dibuat berhasil dan aktif

Gambar 5. Rule berhasil dibuat

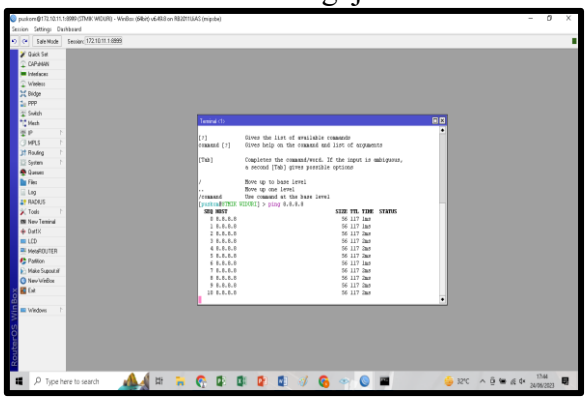


Sumber widuri 2023

2. Pengujian

Berikut pengujian rule yang dibuat untuk mengetahui apakah konfigurasi mikrotik diatas berhasil dan berjalan dengan baik

Gambar 6. Pengujian Rule



Sumber widuri 2023

1. Memastikan bahwa perangkat yang terhubung ke router dapat mengakses internet. Jika perangkat tidak dapat terhubung ke internet, maka ada kemungkinan terdapat kesalahan pada konfigurasi.
2. Melakukan uji coba dengan tab new terminal dimikrotik ketik (ping 8.8.8.8 enter). Jika ping berhasil, maka koneksi antara perangkat dengan router sudah terhubung dengan baik, seperti gambar dibawah ini.

KESIMPULAN DAN SARAN

Perlindungan terhadap akses tidak sah ke layanan jaringan yang sensitif seperti server web, server basis data, dan layanan administrasi, Mencegah kebocoran informasi dan menjaga kerahasiaan, integritas, dan ketersediaan data di jaringan, Pengendalian dan pembatasan akses ke jaringan dan sumber daya yang penting.

Konfigurasi Router MikroTik Saat Ini dan Potensi Celah Keamanan, Diperlukan evaluasi terhadap konfigurasi saat ini pada router MikroTik untuk mengidentifikasi potensi celah keamanan, Perlu memeriksa pengaturan default yang tidak aman, port terbuka yang tidak perlu, dan layanan yang tidak digunakan yang dapat menjadi titik masuk bagi penyerang.

Ancaman Keamanan yang Mungkin Dihadapi oleh Router MikroTik, Ancaman keamanan yang mungkin dihadapi oleh router MikroTik di Laboratorium Komputer meliputi serangan brute force, serangan DDoS, serangan jaringan, dan upaya akses tidak sah, Risiko keamanan juga meliputi pengungkapan informasi sensitif, pemalsuan identitas, dan manipulasi data yang dapat mengancam integritas jaringan.

DAFTAR REFERENSI

Amarudin, A. (2018b). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. Jurnal Teknoinfo, 12(2), 72. https://doi.org/10.33365/jti.v12i2.121

Amarudin. (2018a). Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik Router Menggunakan Metode Port Knocking. Seminar Nasional Sains Dan Teknologi 2018, 1–7.

Amien, J. Al. (2020). Implementasi Keamanan Jaringan Dengan Iptables Sebagai Firewall Menggunakan Metode Port Knocking. Jurnal Fasilkom, 10(2), 159–165. https://doi.org/10.37859/jf.v10i2.2098

Andoro, I. F. B., Agung Budijanto, H., & Aidjili, M. (2022). Analisa Keamanan Jaringan Dengan Mikrotik. RISTEK : Jurnal Riset, Inovasi Dan Teknologi Kabupaten Batang, 6(2), 35–39. https://doi.org/10.55686/ristek.v6i2.111

Brades, T., & Irwansyah. (2022). Pemanfataan Metode Port Knocking Dan Blocking. Seminar Hasil Penelitian Vokasi (SEMHAVOK), 3(No.2), 1–9.

Desmira, D., & Wiryadinata, R. (2022). Rancang Bangun Keamanan Port Secure Shell (SSH) Menggunakan Metode Port Knocking. Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI), 5(1), 28–33. https://doi.org/10.55338/jikomsi.v5i1.242

Haris, A. I., et al. (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

Mikrotik. (2002). Mikrotik. Foundid In 1996, 1. https://mikrotik.com/aboutus

Mulyanto, Y., Julkarnain, M., & Afahar, A. J. (2021). Implementasi Port Knocking Untuk Keamanan Jaringan Smkn 1 Sumbawa Besar. Jinteks, 3(2), 326–335.

Mustofa, T. A., Sutanta, E., & Triyono, J. (2019). Perancangan Dan Implementasi Sistem Monitoring Jaringan Wi-Fi Menggunakan Mikhmon Online Di Wisma Muslim. Jurnal JARKOM, 7(2), 65–76.

n.a. (2019). Router OS Menggunakan Metode Port Knocking Dengan Protokol TCP Dan ICMP Implementation Network Security On Router OS Using The Port Knocking Method With TCP And ICMP Protocols Program Studi D-IV Teknik Informatika.

Rahman, T., et al. (2018). Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking. INOVTEK Polbeng - Seri Informatika, 5(2), 53–64. https://doi.org/10.35314/isi.v5i1.1308

Rahman, T., Sumarna, S., & Nurdin, H. (2020). Analisis Performa Router OS MikroTik pada Jaringan Internet. INOVTEK Polbeng - Seri Informatika, 5(1), 178. https://doi.org/10.35314/isi.v5i1.1308