

Implementasi Keamanan Jaringan Pada Mikrotik Menggunakan Teknik Port Knocking Pada SMK AL - AMIEN

¹Rahmat Dwiyanto, ²Riska Nurtantyo S, ³Iin Kurniasari, ⁴Harso Kurniadi
Teknik Komputer, Universitas Islam Kadiri, Indonesia

rahmatdwiyanto183@gmail.com, riskanurtantyoosarbini@gmail.com,

iin.kurniasari@uniska-kadiri.ac.id, harsokurniadi@uniska-kadiri.ac.id

Submit : 07 Apr 2025 | Diterima : 16 Apr 2025 | Terbit : 17 Apr 2025

ABSTRAK

Dalam digitalisasi yang semakin maju, keamanan jaringan menjadi komponen yang sangat krusial bagi berbagai organisasi maupun institusi pendidikan termasuk SMK AL-AMIEN institusi pendidikan yang mengedepankan penerapan teknologi dalam proses pembelajaran, perlu memastikan bahwa jaringan yang digunakan oleh siswa, guru, dan staf administrasi terlindungi dengan baik. Identifikasi masalah yang terjadi pada jaringan AI AMIEN mencakup beberapa aspek utama, yaitu masalah bandwidth, penyusup, dan monitoring jaringan. Permasalahan bandwidth sering terjadi akibat tingginya jumlah pengguna yang mengakses jaringan untuk mengantisipasi permasalahan pada SMK AI-AMIEN Kediri metode NDLC (*Network Development Life Cycle*) dengan menggunakan penerapan Port Knocking dapat membatasi akses hanya kepada pengguna yang sah, Hasil dari pengujian menunjukkan bahwa keamanan jaringan meningkat setelah implementasi Port Knocking. Berdasarkan pengukuran kualitas layanan (Quality of Service), diperoleh hasil throughput rata-rata sebesar 2673 kbps, delay rata-rata 3 ms, jitter 0 ms, dan packet loss sebesar 0,1%, yang masing-masing mendapatkan nilai indeks 4 dan dikategorikan "Sangat Baik" berdasarkan standar TIPHON. Nilai indeks ratarata sebelum dan sesudah implementasi tetap berada di angka 4, menandakan bahwa penerapan keamanan jaringan tidak menurunkan kualitas layanan. Dengan demikian, implementasi teknik Port Knocking pada Mikrotik terbukti berhasil meningkatkan keamanan jaringan tanpa mengorbankan performa jaringan di SMK AL-AMIEN

Kata kunci: SMK AL-Amien, Port Knocking, Keamanan Jaringan

PENDAHULUAN

Pada era perkembangan teknologi informasi saat ini, setiap mengirimkan suatu pesan informasi menggunakan media internet. Sistem keamanan jaringan komputer harus dilindungi dari serangan dan pemindaian oleh orang yang tidak berhak. Jaringan komputer semakin penting untuk berbagai tujuan, seperti pendidikan, pekerjaan, dan permainan. Karena banyaknya akses ke jaringan, akan ada banyak peluang kejahatan di jaringan atau peretas yang dapat menghancurkan sumber daya server. (Penerapan et al., 2025) Semakin pesat perkembangan teknologi pada setiap waktu, terutama pada bidang telekomunikasi, mulai dari data internet, telephone dan tv kabel. Proses menjalankan layanan - layanan tersebut. (MUSTOFA, 2019) Kemajuan teknologi ini tidak hanya memberikan kemudahan dalam pengelolaan data dan komunikasi, tetapi juga membuka peluang ancaman keamanan yang terus berkembang, untuk mencapai tujuan tersebut penggunaan perangkat keras dan perangkat lunak yang tepat sangatlah penting. Salah satu perangkat lunak yang sering digunakan untuk mengelola jaringan adalah perangkat Mikrotik (Alfiansyah & Sutabri, 2024). sebagai lembaga pendidikan tentunya bertanggung jawab penuh dalam mencerdaskan anak bangsa dalam hal tersebut sudah menjadi kewajiban lembaga pendidikan untuk menyediakan fasilitas penunjang salah satunya jaringan internet untuk membuat interaksi pengguna lebih nyaman, desain jaringan harus dibuat dengan sesuai agar gampang untuk digunakan dan juga kualitas dari keamanan suatu jaringan yang tidak mudah untuk dibobol, sehingga computer network dapat diatur dengan baik (Eka Putra et al., 2024). Salah satu institusi pendidikan yang mengedepankan

penerapan teknologi dalam proses pembelajaran, perlu memastikan bahwa jaringan yang digunakan oleh siswa, guru, dan staf administrasi terlindungi dengan baik. Identifikasi masalah yang terjadi pada jaringan Al Amien mencakup beberapa aspek utama, yaitu masalah bandwidth, penyusup, dan monitoring jaringan. Permasalahan bandwidth sering terjadi akibat tingginya jumlah pengguna yang mengakses jaringan secara bersamaan, menyebabkan kelambatan akses dan ketidakstabilan koneksi. Pengelolaan keamanan jaringan yang efektif tidak hanya penting untuk melindungi data dan informasi sensitif, tetapi juga Akses terbuka yang memungkinkan perangkat asing terhubung ke jaringan dikarenakan tidak adanya keamanan firewall pada router yang menyebabkan lalu lintas jaringan menjadi sibuk dan penggunaan mengakses situs web yang tidak relevan dengan pendidikan untuk memastikan kelancaran operasional sekolah. Hal ini membuktikan bahwa internet berperan aktif dalam aktivitas digital sehari-hari. Dengan adanya hal tersebut maka tentu akan mempermudah ketika ingin melakukan transfer data atau berkomunikasi kepada seseorang selama masih memiliki koneksi dengan internet. (Sari et al., 2022)

Permasalahan tersebutlah peneliti memilih menggunakan metode keamanan jaringan dengan metode Port knocking yang sesuai untuk mengantisipasi permasalahan pada SMK Al-Amien Kediri dapat meningkatkan keamanan jaringan secara signifikan dan menjaga kestabilannya. Hak akses yang lebih terkontrol dan penggunaan bandwidth yang lebih efisien akan mendukung aktivitas pembelajaran berbasis teknologi secara optimal dan menjaga hak akses masuk dan mengurangi lonjakan bandwidth secara signifikan, dengan cara membatasi atau mengurangi hak akses yang tidak diperlukan sehingga dapat menjaga kestabilan pada jaringan SMK Al-Amien.

TINJAUAN PUSTAKA

Jaringan Komputer

Jaringan komputer merupakan suatu sistem yang terdiri dari komputer komputer dan perangkat-perangkat jaringan lainnya yang terhubung satu sama lain, bekerja sama untuk mencapai suatu tujuan. Capaian dari tujuan jaringan komputer adalah setiap bagian dalam jaringan komputer saling memiliki kapabilitas dalam meminta dan memberikan layanan. (Kamila Wilujeng & Voutama, 2024) Informasi berpindah dari komputer ke komputer lainnya dengan menggunakan jaringan daripada melalui perantara manusia, sehingga membuat pertukaran informasi menjadi lebih cepat dan mudah. (Dwipoyono et al., 2023) Pihak yang meminta atau menerima layanan biasa dikenal dengan sebutan client, sementara yang menyediakan atau mengirim layanan disebut dengan server. (Kamila Wilujeng & Voutama, 2024)

Mikrotik

Mikrotik adalah alat untuk menyediakan semua fitur ini dengan instalasi yang cepat dan sederhana serta antarmuka yang mudah digunakan. (Oktaviansyah, 2022) Router mikrotik memiliki kemampuan routing yang canggih, manajemen bandwidth yang kuat, didukung untuk protokol jaringan yang luas, dan memiliki kemampuan mengkonfigurasi sesuai dengan kebutuhan pengguna. Dalam pengelolaan router Mikrotik, keamanan akses ke router menjadi aspek penting yang harus diperhatikan, agar konfigurasi tetap terlindungi dan router aman dari ancaman pihak yang tidak bertanggung jawab untuk melindungi router, diperlukan konfigurasi yang tepat. (Bagus et al., 2025)

Port Knocking

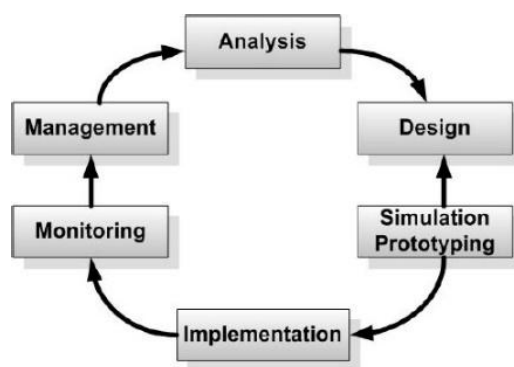
Port knocking merupakan metode yang berfungsi untuk memblokir akses yang tidak diinginkan. Dengan kata lain, jika seseorang perlu mengakses server, mereka harus melakukan ketukan untuk melakukannya, dan port tersebut akan ditutup kembali setelah pengguna selesai menggunakannya. (Eka Putra et al., 2024) Selama urutan ketukan port tidak diketahui, semua port akan tetap tertutup, sehingga membuat server tidak terlihat oleh pemindaian port berbahaya. (Oktaviansyah, 2022). Port knocking akan melakukan penutupan pada port yang tersedia sehingga pengguna tertentu saja yang memiliki hak untuk membuat akses port tersebut dapat mengaksesnya dengan mengetuk terlebih dahulu.

Firewall

Firewall merupakan suatu mekanisme untuk melindungi keamanan jaringan komputer dengan menyaring paket data yang keluar dan masuk di jaringan (Mulyanto & Algi Fari, 2022). Lapisan pertahanan tambahan terhadap potensi ancaman dunia maya. Dengan menerapkan firewall yang efektif, organisasi dapat mengurangi risiko keamanan dan menjaga kelangsungan operasional dan integritas data di lingkungan jaringan mereka. (Cahya et al., 2023)

METODE PENELITIAN

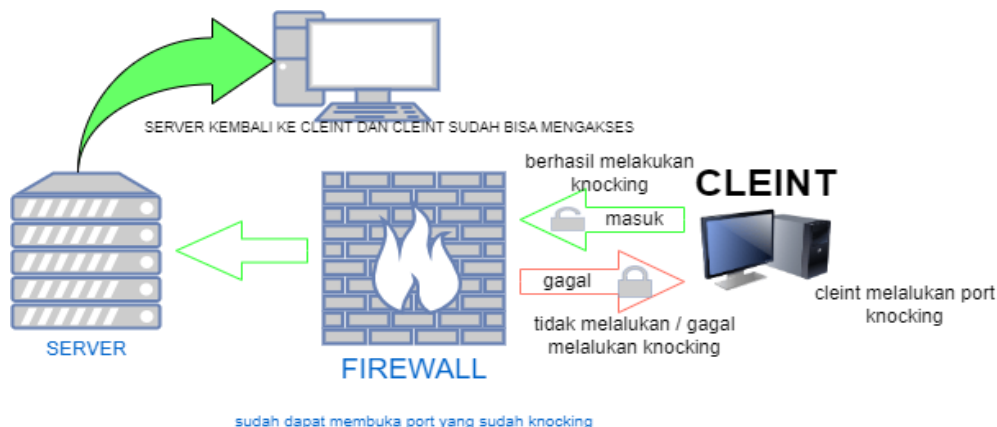
peneliti menganalisis sistem keamanan yang terdapat pada laboratorium TKJ pada SMK Al-Amien untuk mendapatkan data yang valid untuk peneliti, menggunakan metode pendekatan wawancara. Observasi langsung ke objek penelitian, yang bertujuan mendapatkan kondisi lapangan yang sebenarnya dan gambaran keseluruhan, dalam penelitian ini peneliti menggunakan metode NDLC (*Network Development Life Cycle*), Pada tahap ini, kebutuhan-kebutuhan untuk pengembangan sistem jaringan diidentifikasi dan didefinisikan. Tujuan-tujuan yang ingin dicapai serta kriteria-kriteria yang harus dipenuhi oleh sistem dirumuskan dengan jelas. (Eka Putra et al., 2024) Implementasi keamanan port pada mikrotik menggunakan teknik port knocking di SMK Al-Amien Kediri, metode NDLC (*Network Development Life Cycle*) yang merupakan proses perancangan jaringan komputer karena merupakan siklus dari proses membangun hingga mengembangkan jaringan komputer dalam membangun sebuah jaringan komputer dan sebagai acuan yang akan digunakan. (Danil Fajri & Djitalov, 2023) bisa dilihat pada gambar dibawah ini:



Gambar 1 NDLC

Desain Keamanan jaringan

Dengan demikian peneliti akan mengimplementasikan metode *port knocking* dalam rancangan ini untuk meningkatkan keamanan jaringan. Metode ini melakukan pemindaian *port* dan membatasi akses pengguna yang ingin masuk, melindungi sistem dari serangan yang tidak di kenal. Dengan demikian, hanya orang yang telah melakukan *open port knocking* terlebih dahulu akan memiliki akses penuh untuk membuka dan menutup *port*. Bisa dilihat gambar di bawah ini:

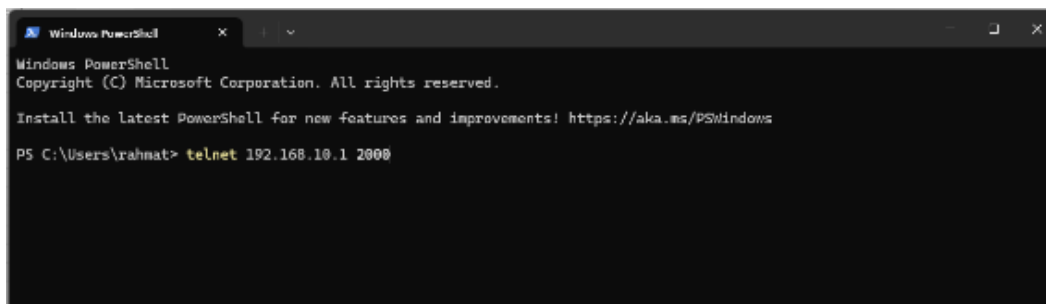


Gambar 2 Firewall

HASIL DAN PEMBAHASAN

Implementasi Port Knocking

Pengujian dilakukan untuk menilai fungsionalitas pada implementasi port. Pengujian dilakukan dengan 2 skenario yaitu ketika implementasi berhasil dan ketika gagal ketika implementasi. Hal pertama untuk melakukan knocking pada mikrotik yaitu siapkan jaringan dari mikrotik dan CMD untuk melakukan knocking ke port yang akan dituju yaitu port 23 contoh seperti berikut :

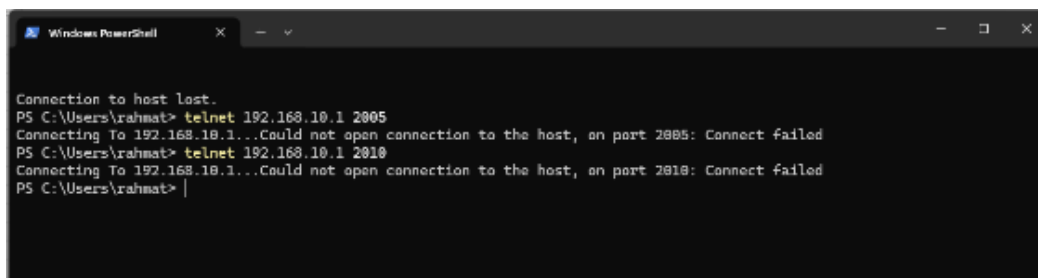


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\rahmat> telnet 192.168.10.1 2000
```

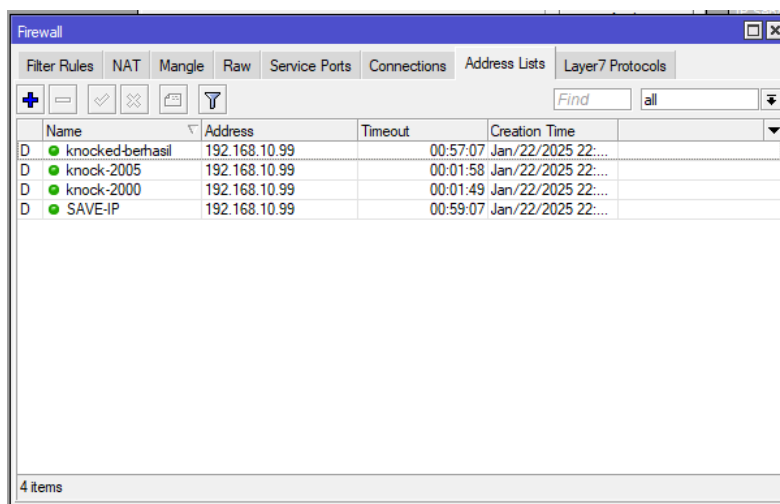
Gambar 3 Melakukan knocking port 2000



```
Windows PowerShell
Connection to host lost.
PS C:\Users\rahmat> telnet 192.168.10.1 2005
Connecting To 192.168.10.1...Could not open connection to the host, on port 2005: Connect failed
PS C:\Users\rahmat> telnet 192.168.10.1 2010
Connecting To 192.168.10.1...Could not open connection to the host, on port 2010: Connect failed
PS C:\Users\rahmat>
```

Gambar 4 Melakukan knocking port 2005 dan 2010

Jika sudah melakukan knocking dengan benar dan berurutan maka kita bisa membuka port 23 dengan aman. Tampilan seperti diatas telah memasuki telnet melewati proses knocking dengan benar. Dan tampilan yang tersimpan di address list di winbox sebagai berikut :

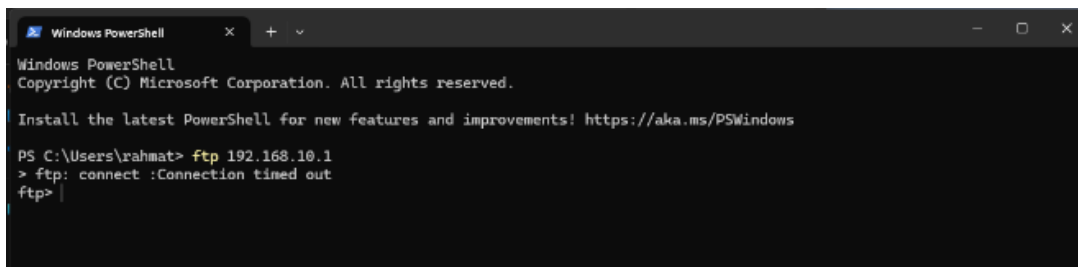


Name	Address	Timeout	Creation Time
knocked-berhasil	192.168.10.99	00:57:07	Jan/22/2025 22:...
knock-2005	192.168.10.99	00:01:58	Jan/22/2025 22:...
knock-2000	192.168.10.99	00:01:49	Jan/22/2025 22:...
SAVE-IP	192.168.10.99	00:59:07	Jan/22/2025 22:...

Gambar 5 Tampilan di address list

Implementasi Tanpa Port Knocking

Gambar di bawah menunjukkan bahwa kita dapat mengakses semua port tanpa harus melalui proses port knocking. Tanpa melakukan ini, tidak ada lapisan keamanan tambahan yang membatasi akses berdasarkan urutan ketukan port. Hal ini dapat membuat sistem lebih rentan terhadap pemindaian dan serangan dari serangan yang tidak diinginkan. Berikut merupakan tampilan port 21 tanpa melakukan knocking terlebih dahulu, hasilnya port tidak mau terbuka dan muncul Connection time out.



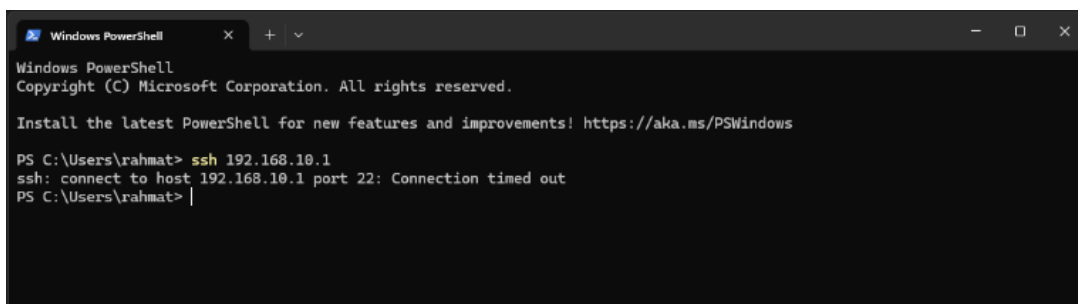
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\rahmat> ftp 192.168.10.1
> ftp: connect :Connection timed out
ftp> |
```

Gambar 6 Tampilan Port 21(ftp) tanpa port knocking

Gambar di bawah menunjukkan bahwa kita dapat mengakses semua port tanpa harus melalui proses port knocking. Berikut merupakan tampilan port 22 tanpa melakukan knocking terlebih dahulu, hasilnya port tidak mau terbuka dan muncul Connection time out.



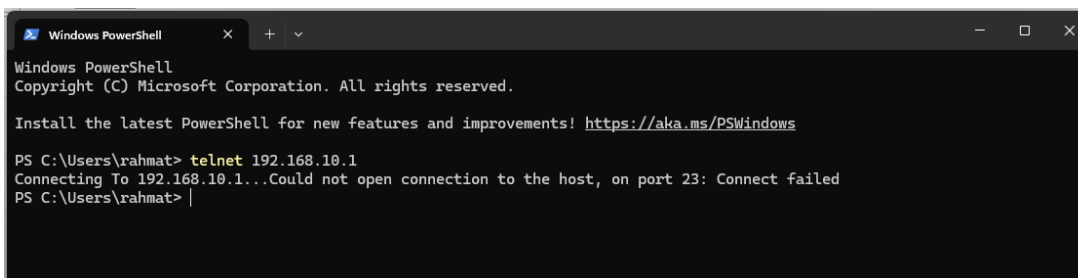
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\rahmat> ssh 192.168.10.1
ssh: connect to host 192.168.10.1 port 22: Connection timed out
PS C:\Users\rahmat> |
```

Gambar 7 Tampilan Port 22(ssh) tanpa port knocking

Gambar di bawah menunjukkan bahwa kita dapat mengakses semua port tanpa harus melalui proses port knocking. Berikut merupakan tampilan port 23 tanpa melakukan knocking terlebih dahulu, hasilnya port tidak mau terbuka dan muncul Could not open connection to the host, on port 23: Connect failed.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

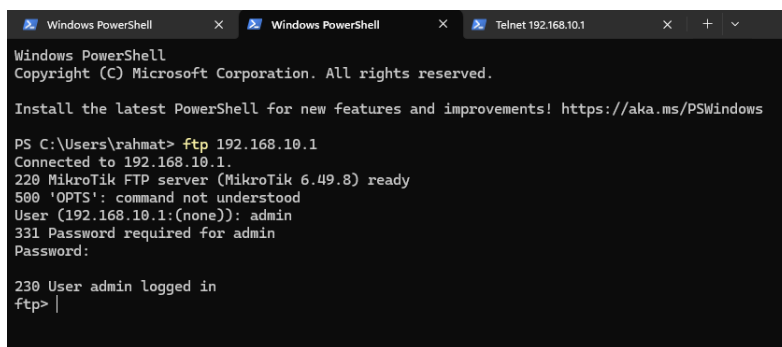
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\rahmat> telnet 192.168.10.1
Connecting To 192.168.10.1...Could not open connection to the host, on port 23: Connect failed
PS C:\Users\rahmat> |
```

Gambar 8 Tampilan Port 23(telnet) tanpa port knocking

Implementasi Dengan Port Knocking

Gambar di bawah menunjukkan bahwa kita dapat mengakses semua port setelah berhasil melakukan port knocking. Dengan metode ini, sistem hanya membuka akses ke port tertentu jika urutan knock yang benar telah dikirim. Ini menambah lapisan keamanan dengan menyembunyikan layanan dari akses langsung oleh pihak yang tidak berwenang. Gambar dibawah menampilkan port 21 dengan melakukan proses knocking terlebih dahulu.



```

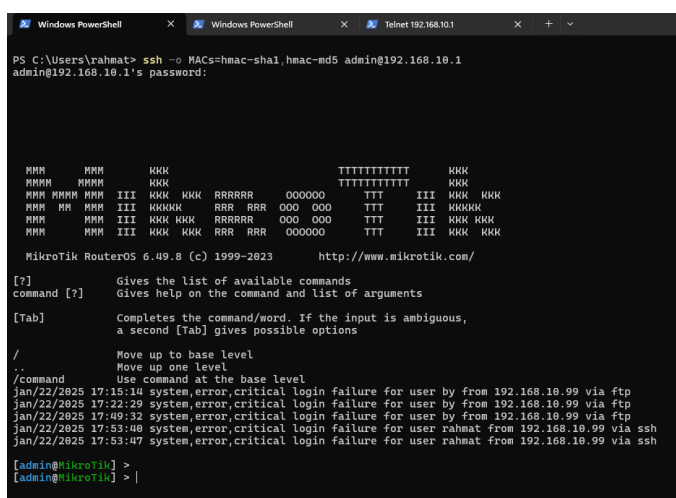
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\rahmat> ftp 192.168.10.1
Connected to 192.168.10.1.
220 MikroTik FTP server (MikroTik 6.49.8) ready
500 'OPTS': command not understood
User (192.168.10.1:(none)): admin
331 Password required for admin
Password:
230 User admin logged in
ftp>
  
```

Gambar 9 Tampilan Port 21(ftp) setelah melakukan knocking

Gambar di bawah menunjukkan bahwa kita dapat mengakses semua port setelah berhasil melakukan port knocking. Dibawah menampilkan port 22 dengan melakukan proses knocking terlebih dahulu.



```

Windows PowerShell
PS C:\Users\rahmat> ssh -o MACs= hmac-sha1,hmac-md5 admin@192.168.10.1
admin@192.168.10.1's password:

MMM   MMM   KKK               TTTTTTTTTT   KKK
MMMM  MMMM  KKK               TTTTTTTTTT   KKK
MMM  MMM  III  KKK  KKK  RRRRRR  OOOOOO  TTT   III  KKK  KKK
MMM  MM   III  KKKKK  RRR  RRR  OOO  OOO  TTT   III  KKKKK
MMM  MM   III  KKK  KKK  RRRRRR  OOO  OOO  TTT   III  KKK  KKK
MMM  MM   III  KKK  KKK  RRR  RRR  OOOOOO  TTT   III  KKK  KKK

MikroTik RouterOS 6.49.8 (c) 1999-2023      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

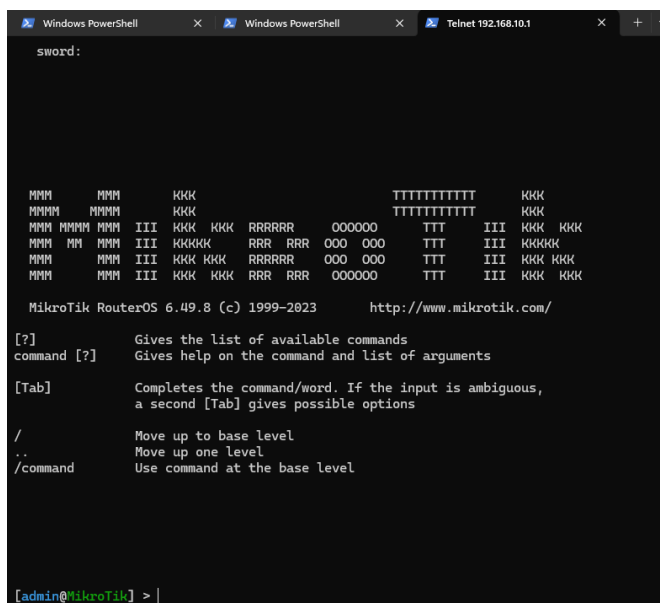
[Tab]        Completes the command/word. If the input is ambiguous,
              a second [Tab] gives possible options

/           Move up to base level
^           Move up one level
/command    Use command at the base level
jan/22/2025 17:15:14 system,error,critical login failure for user by from 192.168.10.99 via ftp
jan/22/2025 17:22:29 system,error,critical login failure for user by from 192.168.10.99 via ftp
jan/22/2025 17:49:32 system,error,critical login failure for user by from 192.168.10.99 via ftp
jan/22/2025 17:53:40 system,error,critical login failure for user rahmat from 192.168.10.99 via ssh
jan/22/2025 17:53:47 system,error,critical login failure for user rahmat from 192.168.10.99 via ssh

[admin@MikroTik] >
[admin@MikroTik] > |
  
```

Gambar 10 Tampilan Port 22(ssh) setelah melakukan knocking

Gambar di bawah menunjukkan bahwa kita dapat mengakses semua port setelah berhasil melakukan port knocking. Dibawah menampilkan port 23 dengan melakukan proses knocking terlebih dahulu.



```

Windows PowerShell
Telnet 192.168.10.1
sword:

MMM   MMM   KKK               TTTTTTTTTT   KKK
MMMM  MMMM  KKK               TTTTTTTTTT   KKK
MMM  MMM  III  KKK  KKK  RRRRRR  OOOOOO  TTT   III  KKK  KKK
MMM  MM   III  KKKKK  RRR  RRR  OOO  OOO  TTT   III  KKKKK
MMM  MM   III  KKK  KKK  RRRRRR  OOO  OOO  TTT   III  KKK  KKK
MMM  MM   III  KKK  KKK  RRR  RRR  OOOOOO  TTT   III  KKK  KKK

MikroTik RouterOS 6.49.8 (c) 1999-2023      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]        Completes the command/word. If the input is ambiguous,
              a second [Tab] gives possible options

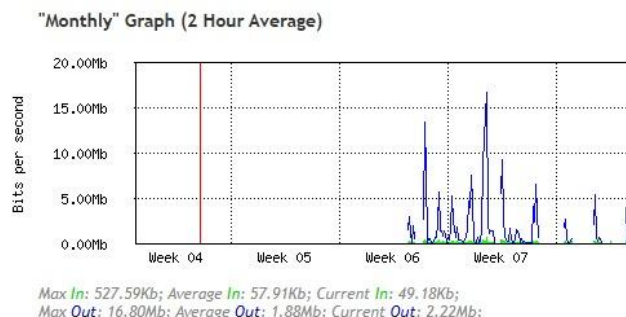
/           Move up to base level
^           Move up one level
/command    Use command at the base level

[admin@MikroTik] > |
  
```

Gambar 11 Tampilan Port 23(telnet) setelah melakukan knocking

Profil Bandwidth Line Rate

Data profile bandwidth line rate ini diambil menggunakan fitur mikrotik *graph* dengan menggunakan ethenet 1. Pada fitur ini kita dapat melihat penggunaan bandwidth dalam bentuk grafik dan gambar di bawah ini merupakan grafik mingguan.



Gambar 12 Grafik penggunaan selama 2 minggu

Pada gambar di atas adalah tampilan total grafik dalam rentan waktu 2 minggu dengan 5 PC dimulai dari tanggal 13 Februari 2025 – 27 Februari 2025.

Tabel 1. Hasil grafik

Waktu	Max Download	Rata-rata Download	Max Upload	Rata-rata Upload
13 Februari 2025-27 Februari 2025	527.59Kb	57.91Kb	16.80Mb	1.88Mb

Pada tabel diatas adalah rata-rata penggunaan bandwidth dalam 2 minggu dimulai dari 13 Februari 2025-27 Februari 2025, dengan jumlah download tertinggi mencapai 527.59Kb dengan rata-rata download 57.91Kb, kemudian upload tertinggi mencapai 16.80Mb dan rata-rata uploadnya 1.88Mb.

Perhitungan Data Sesudah implementasi keamanan jaringan

Berikutnya pengambilan data sesudah implementasi keamanan jaringan menggunakan perhitungan QoS (Quality of Service) yang diperoleh hasil sebagai berikut :

1. Throughput

$$\begin{aligned} \text{Throughput} &= ((\text{Jumlah Data yang Dikirim})/(\text{Lama Waktu Prngiriman data})) \times 8 \\ \text{Throughput} &= (448749460/1342967) \times 8 \\ &= 334,1477936539021 \text{ bytes} \times 8 \\ &= 2.673,182349231217\text{bps} \\ &= 2673 \text{ kbps} \end{aligned}$$

2. Delay

$$\begin{aligned} \text{Delay (s)} &= ((\text{Total Delay})/(\text{Total Paket Yang Diterima})) \times 1000 \\ \text{Delay (s)} &= (1342,855624/441916) \times 1000 \\ &= 3,038712388779768 \times 1000 \\ &= 3,038712 \text{ ms} \end{aligned}$$

3. Jitter

$$\begin{aligned} \text{Jitter} &= ((\text{Total Variasi Delay})/(\text{Total Paket Yang Diterima})) \times 1000 \\ \text{Jitter} &= ((-0,224247)/441916) \times 1000 \\ &= -5,07442590899628 \times 1000 \\ &= -5,074 \text{ ms} \end{aligned}$$

4. Packetloss

$$\begin{aligned} \text{Packet Loss} &= ((\text{Paket Data Yang Dikirim}-\text{Paket Data Yang Diterima}))/(\text{Total Paket Yang Dikirim}) \times 100\% \\ \text{Packet Loss} &= ((441923-441915))/441923 \times 100\% \\ &= (8/441923) \times 100\% \end{aligned}$$

$$= 0,001 \times 100\%$$

$$= 0,1 \%$$

Tabel 1 Hasil Perhitungan Data Sebelum Implementasi Keamanan Jaringan

Parameter	Rerata	Keterangan
	Indeks	Kategori
Troughput	2673 kbps	4 Sangat Baik
Delay	3,0 ms	4 Sangat Baik
Jitter	0 ms	4 Sangat Baik
Packetloss	0,1 %	4 Sangat Baik

Berdasarkan tabel diatas hasil pengukuran meliputi troughput dengan rata – rata 2673 kbps dengan nilai indeks 4 dikategorikan sangat baik, delay dengan rata – rata 3 ms dengan nilai indeks 4 dikategorikan sangat baik, lalu jitter dengan rata – rata 0 ms dengan nilai indeks 4 dikategorikan sangat baik, packetloss dengan rata – rata persentase 0,1% dengan nilai indeks 4 dikategorikan sangat baik.

KESIMPULAN

Implementasi teknik Port Knocking pada Mikrotik di SMK Al-Amien berhasil meningkatkan keamanan jaringan dengan membatasi akses hanya kepada pengguna yang mengetahui ketukan port secara berurutan. Konfigurasi dilakukan dengan menetapkan aturan firewall yang mengharuskan pengguna mengakses serangkaian port dalam urutan yang telah ditentukan sebelum masuk ke port yang diinginkan. Hasil pengujian menunjukkan bahwa hasil pengukuran throughput memiliki rata-rata sebesar 2673 kbps dengan nilai indeks 4, delay rata-rata 3 ms dengan indeks 4, jitter rata-rata 0 ms dengan indeks 4, dan packet loss rata-rata sebesar 0,1% dengan indeks 4, yang semuanya dikategorikan sebagai "Sangat Baik" berdasarkan standar TIPHON. Menurut standar tersebut, kualitas layanan (QoS) dikategorikan sebagai "Sangat Baik" jika memiliki nilai antara 3,8 hingga 4. Sebelum penerapan keamanan jaringan, rata-rata indeks QoS mencapai nilai 4, dan setelah implementasi keamanan jaringan, nilai indeks rata-rata tetap di angka 4. Dengan demikian, dapat disimpulkan bahwa penerapan keamanan jaringan tidak memengaruhi penurunan kualitas layanan, yang tetap berada dalam kategori "Sangat Baik".

Untuk Saran, Pengelola jaringan perlu diberikan pelatihan mengenai konfigurasi dan pengelolaan Port Knocking agar dapat menerapkan dan mengelola jaringan dengan baik. Pemahaman yang baik akan mencegah kesalahan konfigurasi yang dapat menyebabkan jaringan tidak aman dan menghambat kualitas jaringan. Agar pengelolaan jaringan lebih baik lagi, disarankan untuk membuat dokumentasi dan SOP tentang konfigurasi jaringan serta prosedur akses menggunakan Port Knocking. Dengan adanya dokumentasi pengelola jaringan SMK Al-Amien kedepannya dapat lebih mudah memahami sistem yang telah diterapkan.

REFERENSI

- Alfiansyah, M. I., & Sutabri, T. (2024). IJM: Indonesian Journal of Multidisciplinary Analisis Kinerja dan Keamanan Jaringan Menggunakan Perangkat Mikrotik Menggunakan Metode Discovery. *IJM: Indonesian Journal of Multidisciplinary*, 2, 412–419. <https://journal.csspublishing/index.php/ijm>
- Bagus, M. Y., Di, W., & Industri, E. R. A. (2025). *PORT KNOCKING PADA MIKROTIK UNTUK MENINGKATKAN KEAMANAN*. 8, 2115–2122.
- Cahya, B., Rizki, F., Sutiyo, A., Saputra, Y. El, & Elfarizi, M. (2023). Implementasi Firewall Pada Mikrotik Untuk Keamanan Jaringan. *Jurnal JOCOTIS-Journal Science Informatika and Robotics E*, 1(2), 63–80. <https://jurnal.ittc.web.id/index.php/jct/>
- Danil Fajri, R., & Djutalov, R. (2023). Implementasi Jaringan Hotspot Menggunakan Mikrotik untuk RT RW.Net Dengan Menggunakan Metode Network Development Life Cycle (NDLC) Pada Kampung Kelapa Indah Tangerang. *Jurnal Ilmu Komputer Dan Pendidikan*, 1(6), 1437–1444. <https://journal.mediapublikasi.id/index.php/logic>
- Dwipayono, N., Khairil, K., & Sudarsono, A. (2023). Penerapan Firewall Pada Sistem Keamanan

- Jaringan Komputer Di Sekolah Smk Negeri 5 Seluma. *Jurnal Media Infotama*, 19(2), 454–464. <https://doi.org/10.37676/jmi.v19i2.4355>
- Eka Putra, F. P., Amir Hamzah, Agel, W., & Firmansyah Kusuma, R. O. (2024). Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking. *Jurnal Sistim Informasi Dan Teknologi*, 5(4), 82–87. <https://doi.org/10.60083/jsisfotek.v5i4.329>
- Kamila Wilujeng, C., & Voutama, A. (2024). Implementasi Firewall Filter Rules Sebagai Filtering Content Pada Jaringan Komputer Menggunakan Mikrotik. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 8(3), 2680–2685. <https://doi.org/10.36040/jati.v8i3.9530>
- Kurniasari, I., & Wirayudha, M. F. (2025). *Sosialisasi Aplikasi W-JAR sebagai Solusi Persiapan Ujian Kompetensi Keahlian Teknik Komputer Jaringan di SMK Al Amien Kota Kediri*. 7(1), 47–53.
- Mulyanto, Y., & Algi Fari, A. (2022). ANALISIS KEAMANAN LOGIN ROUTER MIKROTIK DARI SERANGAN BRUTEFORCE MENGGUNAKAN METODE PENETRATION TESTING (Studi Kasus: SMK NEGERI 2 SUMBAWA). *Jurnal Informatika, Teknologi Dan Sains*, 4(3), 145–155. <https://doi.org/10.51401/jinteks.v4i3.1897>
- MUSTOFA, I. H. RN Sarbini, H Kurniadi . (2019). Analisa Profil Bandwidth Jaringan Copper, Fiber Optik Dan Migrasi Serta Loss Link Budget Di Pt Telkom Kediri. *Generation Journal*, 3(2), 13. <https://doi.org/10.29407/gj.v3i2.13342>
- Oktaviansyah, P. D. (2022). Penerapan Sistem Pengamanan Port pada Mikrotik Menggunakan Metode Port Knocking. *NetPLG Journal of Network and Computer Applications*, 1(2), 13–24.
- Penerapan, J., Informasi, T., Informasi, F. T., Kristen, U., Wacana, S., & Tengah, J. (2025). *IT-EXPLORE Implementasi port knocking dinamis berbasis waktu pada router untuk pengamanan akses SSH*. 04(52), 106–115. <https://doi.org/10.24246/itexplore.v4i1.2025.pp>
- Sari, I. P., Batubara, I. H., Basri, M., & Hazidar, A. H. (2022). Implementasi Internet of Things Berbasis Website dalam Pemesanan Jasa Rumah Service Teknisi Komputer dan Jaringan Komputer. *Blend Sains Jurnal Teknik*, 1(2), 157–163. <https://doi.org/10.56211/blendsains.v1i2.136>