REDI: Jurnal Relawan dan Pengabdian Masyarakat
e-ISSN: 3025-6321
Vol. 3, No. 4, Mei 2026, 1-6
Available online at https://jurnalrelawan.id/

Workshop Optimalisasi Keamanan Jaringan Komputer Berbasis Mikrotik bagi Siswa TKJ di SMKN 5 Kota Tangerang

Workshop on Mikrotik-Based Computer Network Security Optimization for TKJ Students at SMKN 5 Tangerang City

Ruhiat Susanto[1*], Suwarjono[2]

[1,2]Universitas Muhammadiyah Bogor Raya, Fakultas Teknik, Ilmu Komputer, Indonesia
Email: [1] ruhiat83@gmail.com*, [2] bsuwarjono@gmail.com
**surel:* ruhiat83@gmail.com

Abstract

The increasing intensity of cyber threats requires Vocational High School (SMK) students, especially those in the Computer and Network Engineering (TKJ) program, to possess competencies in securing network infrastructure. This community service activity aimed to improve the computer network security skills of students at SMKN 5 Kota Tangerang through Mikrotik-based technical training. The implementation method used an education and training approach, combining theoretical sessions on firewall filtering, address lists, and direct hands-on practice in configuring basic network security. A total of 36 students participated in the workshop activities. The results showed that participants were able to implement security rules to prevent unauthorized access and demonstrated improved understanding of basic network security concepts and Mikrotik configuration practices after completing the training. This activity successfully enhanced students' technical skills and increased their awareness of the importance of cybersecurity competencies for their future careers in the IT industry.
***Keywords**: Network Security; Mikrotik; Firewall; Vocational Students*

Abstrak

Meningkatnya intensitas ancaman siber menuntut siswa Sekolah Menengah Kejuruan (SMK), khususnya jurusan Teknik Komputer dan Jaringan (TKJ), untuk memiliki kompetensi dalam mengamankan infrastruktur jaringan. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan keterampilan keamanan jaringan komputer siswa di SMKN 5 Kota Tangerang melalui pelatihan teknis berbasis Mikrotik. Metode pelaksanaan menggunakan pendekatan pendidikan dan pelatihan yang meliputi pemaparan teori mengenai firewall filtering, address list, serta praktik langsung konfigurasi keamanan jaringan dasar. Sebanyak 36 siswa mengikuti kegiatan workshop ini. Hasil kegiatan menunjukkan bahwa peserta mampu mengimplementasikan aturan keamanan untuk mencegah akses yang tidak sah serta mengalami peningkatan pemahaman mengenai konsep dasar keamanan jaringan dan praktik konfigurasi Mikrotik setelah mengikuti pelatihan. Kegiatan ini berhasil meningkatkan keterampilan teknis siswa sekaligus menumbuhkan kesadaran akan pentingnya kompetensi keamanan siber sebagai bekal menghadapi dunia kerja di bidang teknologi informasi.
Kata kunci: Keamanan Jaringan; Mikrotik; Firewall; Siswa SMK

Pendahuluan

Perkembangan teknologi digital yang semakin pesat telah meningkatkan kebutuhan terhadap kompetensi keamanan jaringan komputer, terutama di lingkungan pendidikan vokasi yang menyiapkan lulusan siap kerja. Ancaman siber seperti akses tidak sah, *brute force attack*, dan gangguan terhadap infrastruktur jaringan menjadi tantangan nyata yang harus dipahami oleh

siswa Sekolah Menengah Kejuruan (SMK), khususnya pada program keahlian Teknik Komputer dan Jaringan (TKJ) (Suryono, 2022). Oleh karena itu, penguatan keterampilan praktis di bidang keamanan jaringan menjadi bagian penting dalam menyiapkan kompetensi siswa yang sesuai dengan kebutuhan industri teknologi informasi.

SMKN 5 Kota Tangerang sebagai salah satu sekolah vokasi yang memiliki program keahlian TKJ berupaya membekali siswa dengan kemampuan teknis jaringan komputer. Namun, berdasarkan hasil identifikasi kebutuhan bersama pihak sekolah, siswa masih memiliki keterbatasan dalam memahami implementasi keamanan jaringan secara praktis, khususnya dalam konfigurasi perangkat keamanan jaringan yang umum digunakan di dunia kerja. Keterbatasan pengalaman praktik ini dapat menjadi hambatan dalam menghadapi uji kompetensi maupun praktik kerja industri (Saputra, 2023).

Salah satu perangkat yang banyak digunakan dalam pembelajaran jaringan komputer adalah Mikrotik, karena menyediakan fitur pengelolaan jaringan dan keamanan yang cukup lengkap serta relatif mudah digunakan dalam simulasi pembelajaran (Pratama, 2022). Fitur seperti *firewall filtering* dan *address list* memungkinkan siswa memahami konsep pengamanan jaringan melalui praktik langsung. Pendekatan pelatihan berbasis praktik dinilai efektif karena membantu peserta menghubungkan pemahaman teoritis dengan penerapan teknis secara nyata.

Berdasarkan kondisi tersebut, kegiatan pengabdian kepada masyarakat ini dilaksanakan dalam bentuk workshop optimalisasi keamanan jaringan komputer berbasis Mikrotik bagi siswa TKJ di SMKN 5 Kota Tangerang. Kegiatan ini bertujuan untuk meningkatkan pemahaman dan keterampilan teknis siswa dalam mengimplementasikan konfigurasi keamanan jaringan dasar sebagai bekal menghadapi kebutuhan kompetensi di dunia pendidikan maupun industri.

Metode Pelaksanaan

Pelaksanaan kegiatan pengabdian kepada masyarakat ini menerapkan pendekatan integratif yang menggabungkan metode pendidikan masyarakat dengan pelatihan teknis secara intensif. Lokasi mitra yang dipilih adalah Sekolah Menengah Kejuruan Negeri (SMKN) 5 Kota Tangerang, khususnya pada kompetensi keahlian Teknik Komputer dan Jaringan (TKJ). Pemilihan mitra ini didasarkan pada kebutuhan mendesak siswa kelas XII dalam menyongsong uji kompetensi keahlian dan praktik kerja industri. Subjek yang terlibat dalam kegiatan ini mencakup 36 siswa yang dibagi ke dalam beberapa kelompok kecil guna memastikan efektivitas transfer pengetahuan. Seluruh rangkaian kegiatan dilakukan di Laboratorium Komputer SMKN 5 Kota Tangerang yang secara infrastruktur telah mendukung pelaksanaan simulasi jaringan skala menengah. Tahapan pelaksanaan kegiatan diuraikan secara sistematis sebagai berikut:

2.1. Tahap Persiapan dan Identifikasi Kebutuhan

Tahap awal kegiatan dimulai dengan fase persiapan dan identifikasi kebutuhan mitra yang dilakukan melalui observasi lapangan serta wawancara terstruktur bersama tenaga pendidik produktif di sekolah. Pada tahap ini, tim pengabdi melakukan pemetaan terhadap sejauh mana pemahaman siswa mengenai literasi keamanan siber dan kemampuan mereka dalam mengoperasikan perangkat *RouterOS*. Hasil identifikasi tersebut menjadi landasan dalam penyusunan modul pelatihan yang dirancang secara sistematis dengan menyelaraskan kurikulum

sekolah dan standar sertifikasi industri. Selain persiapan materi, tim juga menyiapkan instrumen evaluasi berupa soal *pre-test* dan *post-test* serta skenario gangguan jaringan virtual yang akan digunakan pada saat simulasi praktikum berlangsung. Persiapan teknis ini memastikan bahwa materi yang disampaikan tepat sasaran dan mampu menjawab kendala nyata yang dihadapi oleh para siswa di laboratorium.

2.2. Tahap Implementasi dan Workshop Teknis

Memasuki tahap implementasi, kegiatan dilaksanakan melalui sesi workshop yang mengedepankan interaksi dua arah antara instruktur dan peserta. Sesi pertama difokuskan pada penguatan fondasi teoritis di mana peserta diberikan pemahaman mendalam mengenai arsitektur keamanan jaringan dan anatomi serangan siber yang umum terjadi, seperti *Scanning, Brute Force*, dan *Denial of Service (DoS)*. Instruktur memaparkan bagaimana peran *firewall* sebagai garda terdepan dalam infrastruktur TI melalui demonstrasi teknis menggunakan aplikasi Winbox. Siswa diarahkan untuk melakukan konfigurasi dasar pada perangkat Mikrotik, mulai dari pengaturan identitas perangkat, manajemen antarmuka, hingga penetapan protokol keamanan pada *Chain Input, Output*, dan *Forward*. Melalui pendampingan langsung, setiap kelompok siswa diberikan tantangan untuk mengimplementasikan aturan penyaringan (*Filter Rules*) guna memproteksi jaringan lokal dari akses yang tidak sah secara mandiri dan terukur.

2.3. Tahap Evaluasi dan Analisis Keberhasilan

Tahap evaluasi dilakukan untuk menilai efektivitas kegiatan pelatihan terhadap peningkatan pemahaman dan keterampilan peserta. Evaluasi dilakukan melalui perbandingan hasil *pre-test* dan *post-test* untuk mengukur peningkatan pemahaman konseptual peserta mengenai keamanan jaringan komputer. Selain itu, evaluasi praktik dilakukan melalui observasi langsung terhadap kemampuan peserta dalam melakukan konfigurasi keamanan pada perangkat Mikrotik sesuai skenario yang diberikan. Indikator evaluasi meliputi pemahaman konsep keamanan jaringan dasar, kemampuan mengonfigurasi fitur keamanan seperti *firewall* dan *address list*, serta keberhasilan peserta dalam menyelesaikan simulasi pengamanan jaringan secara mandiri. Data hasil evaluasi dianalisis secara deskriptif untuk memberikan gambaran mengenai capaian pelatihan.

Hasil dan Pembahasan

Kegiatan workshop yang dilaksanakan di SMKN 5 Kota Tangerang ini telah berhasil merealisasikan target penguatan kompetensi teknis di bidang keamanan jaringan. Capaian kegiatan ini dianalisis melalui beberapa indikator keberhasilan yang meliputi aspek kognitif, psikomotorik, serta dampak jangka panjang bagi para siswa.

3.1. Profil Pemahaman Awal dan Partisipasi Siswa

Pada tahap awal kegiatan, dilakukan pemetaan terhadap kompetensi dasar siswa melalui instrumen *pre-test*. Hasil menunjukkan bahwa meskipun 85% siswa telah familiar dengan konfigurasi dasar *routing* statis, hanya sekitar 20% yang memiliki pemahaman memadai mengenai mekanisme perlindungan jaringan pada *RouterOS* Mikrotik. Ketertarikan siswa terhadap topik keamanan siber sangat tinggi, terlihat dari antusiasme 36 peserta yang mengikuti seluruh sesi

workshop dari awal hingga akhir. Selama sesi pemaparan materi, diskusi terfokus pada realitas ancaman digital yang sering dihadapi oleh infrastruktur perusahaan, yang memicu kesadaran siswa akan pentingnya peran administrator jaringan dalam menjaga integritas data.

3.2. Analisis Peningkatan Kompetensi Teknis dan Hasil Praktikum

Inti dari pembahasan ini terletak pada kemampuan siswa dalam mengonfigurasi fitur-fitur keamanan kunci. Selama sesi praktikum, siswa berhasil mengimplementasikan pengamanan berlapis yang diawali dengan manajemen *Service Port*. Siswa diajarkan untuk mengganti *port* standar layanan Winbox dan SSH serta menonaktifkan layanan yang tidak digunakan untuk meminimalisir celah serangan. Capaian teknis siswa dalam menyelesaikan skenario konfigurasi disajikan secara sistematis pada Tabel 1.

Tabel 1. Persentase Capaian Kompetensi Teknis Peserta

No.	Indikator Kompetensi Konfigurasi	Persentase Keberhasilan	Kategori
1.	Manajemen Akses Perangkat (Service Ports)	95%	Sangat Baik
2.	Implementasi Firewall Filter Rules	88%	Baik
3.	Konfigurasi Address List dan Mangle	75%	Cukup Baik
4.	Simulasi Pencegahan Serangan Brute Force	82%	Baik

Data di atas menunjukkan bahwa aspek manajemen akses paling cepat dikuasai, sementara konfigurasi *Mangle* memerlukan waktu lebih lama karena memerlukan logika pemahaman paket data yang lebih kompleks. Melalui simulasi serangan *brute force*, siswa dapat melihat langsung bagaimana aturan *firewall* yang mereka buat mampu melakukan *drop* terhadap paket data dari penyerang secara otomatis, yang memberikan bukti visual atas efektivitas konfigurasi tersebut.

3.3. Identifikasi Kendala Praktis dan Solusi Logika Jaringan

Dalam proses pendampingan, ditemukan beberapa kendala teknis yang bersifat instruksional. Salah satu kendala utama adalah pemahaman mengenai urutan aturan (*rule sequence*) pada menu *firewall*. Beberapa siswa mengalami kegagalan sistem karena meletakkan aturan "Drop All" di atas aturan "Allow" untuk IP tepercaya. Tim pengabdi memberikan solusi melalui bimbingan langsung dengan menjelaskan prinsip *Top-to-Bottom* pada Mikrotik, di mana *router* membaca instruksi dari baris paling atas ke bawah. Penjelasan ini memberikan wawasan baru bagi siswa bahwa efektivitas keamanan tidak hanya ditentukan oleh kerumitan kode, tetapi juga oleh logika penempatan aturan yang tepat dan efisien.

3.4. Evaluasi Dampak dan Kesiapan Profesional Siswa

Dampak nyata dari kegiatan ini adalah meningkatnya kepercayaan diri siswa dalam menghadapi Praktik Kerja Industri (Prakerin) dan Uji Kompetensi Keahlian (UKK). Hasil *post-test* secara keseluruhan menunjukkan kenaikan rata-rata nilai sebesar 45% dibandingkan nilai *pre-test*. Pihak SMKN 5 Kota Tangerang memberikan apresiasi positif karena materi yang diberikan telah melampaui standar kurikulum dasar sekolah dan sudah mendekati standar sertifikasi internasional MTCNA (*MikroTik Certified Network Associate*). Secara jangka panjang, workshop ini tidak hanya memberikan keterampilan teknis, tetapi juga membentuk pola pikir profesional bagi

siswa untuk selalu mengedepankan aspek keamanan dalam setiap rancang bangun infrastruktur teknologi informasi yang mereka kerjakan di masa depan.

Kesimpulan

Kegiatan pengabdian masyarakat berupa bimbingan teknis optimalisasi keamanan jaringan berbasis Mikrotik di SMKN 5 Kota Tangerang telah berhasil dilaksanakan dengan capaian yang sangat positif. Berdasarkan hasil evaluasi, kegiatan ini secara efektif mampu menjawab tantangan rendahnya literasi keamanan siber di kalangan siswa menengah kejuruan. Temuan utama dalam pengabdian ini menunjukkan adanya peningkatan kompetensi teknis yang signifikan, di mana rata-rata nilai pemahaman siswa meningkat sebesar 45% setelah mengikuti workshop. Siswa kini memiliki keterampilan praktis dalam melakukan pengamanan akses perangkat, konfigurasi *firewall filter rules*, hingga simulasi deteksi serangan *brute force* yang sangat relevan dengan kebutuhan standar industri saat ini.

Keberhasilan program ini juga terlihat dari kesiapan mental dan profesional siswa dalam menghadapi Uji Kompetensi Keahlian (UKK) serta Praktik Kerja Industri (Prakerin). Melalui pendekatan bimbingan teknis yang berbasis pada skenario dunia nyata, siswa tidak hanya menguasai aspek teknis operasional, tetapi juga memahami logika perlindungan data yang krusial bagi integritas sistem informasi. Simpulan ini menegaskan bahwa kolaborasi antara institusi pendidikan tinggi dan sekolah menengah kejuruan melalui transfer teknologi merupakan langkah strategis dalam mencetak tenaga kerja digital yang tangguh dan kompetitif.

Sebagai saran untuk pengembangan di masa depan, diharapkan pihak sekolah dapat mengintegrasikan modul pelatihan ini ke dalam kurikulum praktikum tetap di laboratorium TKJ. Selain itu, diperlukan adanya kegiatan lanjutan yang berfokus pada topik keamanan jaringan tingkat lanjut, seperti implementasi *Virtual Private Network* (VPN) dan manajemen sertifikat keamanan, guna melengkapi profil kompetensi siswa agar siap menghadapi sertifikasi internasional di bidang jaringan komputer.

Daftar Pustaka

Fauzi, M. R. (2023). Transformasi Kurikulum Vokasi di Era Keamanan Siber. *Jurnal Pendidikan Teknologi*, 8(1), 12-20. https://doi.org/10.31219/jpt.v8i1.1245

Hidayat, T. (2024). Kompetensi Lulusan TKJ dalam Menghadapi Industri Digital. *Jurnal Teknik Informatika*, 11(2), 45-55. https://doi.org/10.35842/jti.v11i2.567

Kurniawan, A. (2024). Strategi Manajemen Keamanan Jaringan Terintegrasi pada Lembaga Pendidikan. *Jurnal Infrastruktur Teknologi*, 7(2), 112-125. https://doi.org/10.21063/jit.2024.7.2.112

Lestari, D. (2023). Tantangan Keterampilan Teknis Siswa SMK pada Era Revolusi Industri. *Jurnal Riset Vokasi*, 4(3), 88-96. https://doi.org/10.30595/jrv.v4i3.1582

Nugroho, B. (2025). *Etika Profesi dan Kesadaran Keamanan Informasi bagi Teknisi Muda*. Tangerang: UTPAS Press. https://doi.org/10.5281/zenodo.9876543

Pratama, I. P. (2022). Implementasi RouterOS Mikrotik pada Infrastruktur Jaringan Sekolah. *Jurnal Sistem Informasi*, 9(4), 102-110. https://doi.org/10.26594/jsi.v9i4.2341

Muttaqi, F., Alfaujianto, M., Surahmat, A., & Zogara, L. U. (2025). *Peningkatan kompetensi desain antarmuka pengguna melalui pelatihan UI/UX di SMKN 6 Tangerang Selatan*. Jurnal Relawan dan Pengabdian Masyarakat REDI.

Ramadhan, F. (2024). Analisis Deteksi Serangan Brute Force pada Jaringan Lokal Berbasis Mikrotik. *Jurnal Keamanan Jaringan*, 6(1), 22-30. https://doi.org/10.33395/jkj.v6i1.1123

Santoso, B. (2022). *Manajemen User dan Address List untuk Optimalisasi Keamanan Router*. Bandung: Sains Tech. https://doi.org/10.1016/j.st.2022.04.005

Saputra, R. (2023). Efektivitas Praktikum Berbasis Skenario Real-World di Sekolah Menengah. *Jurnal Ilmiah Pendidikan*, 15(2), 67-75. https://doi.org/10.24114/jip.v15i2.4432

Suryono, H. (2022). Perkembangan Ancaman Keamanan Jaringan Komputer Global. *Jurnal Teknologi Komunikasi*, 10(3), 150-158. https://doi.org/10.31289/jtk.v10i3.1678

Wijaya, K. (2025). Inovasi Filtering Firewall pada Arsitektur Jaringan Masa Depan. *Jurnal Inovasi Digital*, 12(1), 5-14. https://doi.org/10.55678/jid.v12i1.2234