ABDITEKNIKA
Jurnal Pengabdian Kepada Masyarakat
Volume 5 Nomor 2 Oktober 2025 Halaman 98-103
DOI : https://doi.org/10.31294/abditeknika.v5i2.9637 ISSN 2775-1694

Pentingnya Kesadaran Keamanan Siber Melalui Pemanfaatan Teknologi VPN dan Pemahaman Enkripsi untuk Perlindungan Data

Aditya Lukmana[1*], Asep Amril Rudiyat[2], Enpri Rifa Azima[3], Muhammad Thariq Azmi[4], Arief Zulianto[5]

[1,2,3,4,5] Universitas Langlangbuana
Jl. Karapitan No.116, Cikawao, Kec. Lengkong, Kota Bandung, Jawa Barat 40261, Indonesia

email korespondensi: lukmana56@gmail.com

Submit: 26-07-2025 | Revisi : 11-08-2025 | Terima : 03-09-2025 | Terbit Online : 03-10-2025

Abstrak
Transformasi digital yang pesat menuntut peningkatan literasi keamanan siber, khususnya di lingkungan akademik. Program pengabdian ini dilaksanakan untuk menjawab tantangan kurangnya kesadaran dan keterampilan Civitas Akademika Universitas Muhammadiyah Ahmad Dahlan Cirebon dalam menggunakan teknologi jaringan yang aman. Masalah ini diidentifikasi melalui observasi awal, di mana meskipun penggunaan internet dan perangkat digital meluas, pemahaman mendalam tentang konsep keamanan jaringan dan *VPN* masih terbatas. Melalui pelatihan intensif yang mencakup pengenalan dasar keamanan jaringan, jenis-jenis *Virtual Private Network (VPN)* seperti *L2TP*, *IPsec*, dan *WireGuard*, serta praktik konfigurasi, program ini berhasil meningkatkan pemahaman dan keterampilan peserta. Evaluasi pre-test dan post-test menunjukkan peningkatan skor sebesar 31,35%. Selain itu, lebih dari 75% peserta mampu mengaplikasikan VPN dalam aktivitas harian. Pelatihan ini membuktikan bahwa pendekatan edukatif berbasis praktik mampu meningkatkan kesadaran siber dan memberikan dampak nyata terhadap keamanan digital di lingkungan akademik.

Kata Kunci : Keamanan Siber; VPN; Enkripsi

Abstract
The rapid digital transformation necessitates an increase in cybersecurity literacy, particularly in academic environments. This community service program was conducted to address the challenge of a lack of awareness and skills among the academic community of Universitas Muhammadiyah Ahmad Dahlan Cirebon in using secure network technology. This problem was identified through initial observations, which found that despite the widespread use of the internet and digital devices, an in-depth understanding of network security concepts and VPNs was still limited. Through intensive training that included an introduction to network security fundamentals, different types of Virtual Private Networks (VPNs) such as L2TP, IPsec, and WireGuard, and configuration practices, the program successfully improved participants' understanding and skills. The evaluation of pre-tests and post-tests showed a score increase of 31.35%. Additionally, more than 75% of participants were able to apply VPNs in their daily activities. This training proves that a practice-based educational approach can increase cyber awareness and provide a tangible impact on digital security in the academic environment.

Keywords : Cybersecurity; VPN; Encryption

1. Pendahuluan

Kondisi masyarakat di era digital saat ini menuntut setiap individu dan organisasi untuk memiliki kemampuan adaptasi terhadap perkembangan teknologi informasi dan keamanan siber. Manusia secara umum memiliki gaya hidup baru yang tidak bisa dilepaskan dari perangkat yang serba elektronik (Rorong & Londa, 2020). Keamanan data pribadi menjadi semakin penting di tengah ancaman siber yang terus berkembang (Siaulhak et al., 2024). Serangan keamanan pada jaringan komputer maupun internet terjadi karena adanya kejahatan dunia maya (*cybercrime*) . Jenis-jenis serangan keamanan yang mungkin terjadi misalnya adalah sniffing, spoofing, Denial of Service (DoS), Session Hijacking dan lain-lain (Widya Sari, 2011)

Banyak permasalahan yang muncul di lingkungan sekitar masyarakat modern, seperti rendahnya literasi digital mengenai keamanan dan kurangnya pemanfaatan teknologi informasi secara aman untuk mendukung aktivitas sehari-hari. Keamanan jaringan menjadi hal yang sangat krusial, terutama dalam menghadapi potensi ancaman serangan oleh peretas yang bertujuan untuk mencuri data sensitif, mengganggu layanan, atau bahkan merusak reputasi institusi (Muhamad Malik Matin et al., 2024a). Keamanan jaringan didefinisikan sebagai sebuah

perlindungan dari sumber daya terhadap upaya penyingkapan, modifikasi, utilisasi, pelarangan dan perusakan oleh person yang tidak diijinkan (Pratama Putra, 2016). Observasi awal di lingkungan Universitas Muhammadiyah Ahmad Dahlan Cirebon, mencakup mahasiswa, tenaga kependidikan, dan staf IT, menunjukkan bahwa meskipun penggunaan internet dan perangkat digital telah meluas, pemahaman mendalam tentang konsep keamanan jaringan, khususnya *Virtual Private Network (VPN),* masih terbatas.

Sebagai contoh, civitas akademika seringkali mengakses jaringan universitas atau informasi sensitif melalui koneksi yang tidak terenkripsi atau kurang aman, dan harus dilakukan dengan adanya pengamanan data. Pengaman data ini melakukan perlindungan terhadap data dari berbagai ancaman seperti kebocoran, kerusakan, atau akses yang tidak sah (Aditya et al., 2024). Pada kasus lain, saat ini banyak orang yang menggunakan aplikasi web untuk produk atau jasa yang diinginkan. Pengguna yang memberikan nama, data-data pribadi, data pembayaran, bisa menjadi sumber penghasilan bagi para *hacker* yang menarget informasi rahasia pengguna (Prasetyo et al., 2024)

Berdasarkan analisis situasi yang telah dilakukan, beberapa permasalahan konkret dan mendesak yang dihadapi oleh Civitas Akademika Universitas Muhammadiyah Ahmad Dahlan Cirebon dapat diidentifikasi. Permasalahan ini secara langsung memengaruhi efektivitas operasional dan kemampuan adaptasi digital mereka dalam konteks keamanan. Kurangnya pemahaman tentang konsep keamanan jaringan, keamanan dalam bertansaksi dan belum memahami bagaimana cara menggunakan penggunaan *VPN* secara umum di kalangan civitas akademika. Banyak di antara mereka yang belum terbiasa dengan pentingnya enkripsi dan *tunneling* yang aman dalam berinteraksi di dunia maya.

Terdapat keterbatasan pengetahuan mengenai jenis-jenis *VPN* yang berbeda, seperti *L2TP* (*Layer 2 Tunneling Protocol*) adalah salah satu protocol tunneling yang bias digunakan dan mendukung *VPN* (Sumarna & Maulana, 2021), *IPsec* (*Internet Protocol Security*) yaitu sebuah protokol enkripsi yang menyediakan transmisi data terenkripsi yang aman pada network layer dalam jaringan (Muhamad Malik Matin et al., 2024b , dan *WireGuard* adalah salah satu tipe *VPN* yang sederhana namun cepat, aman dan modern (Novianto et al., 2022), serta perbedaan karakteristik dan skenario penggunaannya. Secara garis besar *VPN* adalah suatu jaringan lokal yang terhubung melalui media jaringan publik (Dewi et al., 2020).

Menanggapi permasalahan yang teridentifikasi di Civitas Akademika Universitas Muhammadiyah Ahmad Dahlan Cirebon, tim pengabdian merumuskan serangkaian solusi yang terstruktur dan terarah. Solusi utama yang ditawarkan adalah penyelenggaraan program pelatihan intensif yang berfokus pada pemanfaatan teknologi informasi dan keamanan jaringan, khususnya *VPN (L2TP, IPsec, WireGuard)*, untuk meningkatkan keterampilan digital yang aman. Pelatihan ini dirancang secara ilmiah dan praktis, dengan tujuan memberikan pengetahuan dan keterampilan yang dapat langsung diterapkan oleh peserta dalam tugas-tugas sehari-hari mereka, terutama dalam menjaga hak privasi, dimana hak privasi adalah hak asasi setiap individu untuk menjaga kerahasiaan dan keamanan data pribadi mereka (Anggen Suari & Sarjana, 2023).

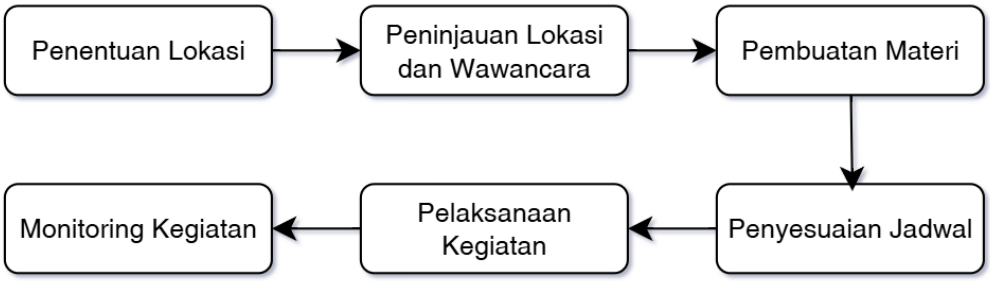
Setiap solusi dirancang untuk secara langsung mengatasi permasalahan spesifik yang ada. Misalnya, untuk mengatasi kurangnya pengenalan terhadap konsep keamanan jaringan dan *VPN*, pelatihan akan dimulai dengan pengetahuan mengenai jenis-jenis serangan siber, jenis enkripsi, jenis *virtual private network* dan mengapa koneksi aman itu penting. Pada akhir materi ditampilkan juga demo penggunaan *VPN* dan *Tunneling*. Selanjutnya, untuk mengatasi keterbatasan pemahaman jenis-jenis *VPN*, modul pelatihan akan mencakup sesi khusus tentang *L2TP, IPsec, dan WireGuard*. Materi pelatihan disusun secara bertahap, mulai dari teori dasar hingga praktik langsung, dengan tujuan memastikan peserta tidak hanya memahami konsep, tetapi juga dapat menerapkannya dalam praktik (Pelatihan Dasar Jaringan Komputer bagi Pemula et al., 2024)

2. Metode

Dalam penentuan materi, tim melakukan peninjauan lokasi dan wawancara dengan perwakilan mitra untuk mendapatkan data mengenai kondisi dan kebutuhan spesifik, serta mengonfirmasi permasalahan yang ada. Selain itu, untuk mengukur keberhasilan program, digunakan pre-test dan post-test. Alat ukur keberhasilan lainnya mencakup observasi langsung terhadap perubahan sikap dan kemampuan peserta, serta pengumpulan umpan balik (*feedback*) melalui kuesioner. Teknik-teknik ini dirancang untuk memastikan transfer pengetahuan dan keterampilan yang efektif kepada peserta

Dalam pelaksanaan kegiatan pengabdian kepada masyarakat ini menggunakan metode yang partisipatif dan praktis. Partisipatif mengandung arti ikut sertanya peserta didik didalam kegiatan pembelajaran (Alisalman, 2022), kemudian dirancang untuk memastikan transfer pengetahuan dan keterampilan yang efektif kepada peserta. Metode utama yang diterapkan adalah kombinasi pemberian materi, demo aplikasi, dan praktik langsung, mirip dengan pendekatan yang terbukti efektif dalam peningkatan kemampuan melalui simulasi. Pendekatan ini dipilih karena peserta cenderung lebih menyukai pembelajaran yang melibatkan partisipasi aktif dibandingkan ceramah. Langkah-langkah kerja yang ditempuh meliputi:

1. Penentuan lokasi kegiatan, yaitu Kampus Universitas Muhammadiyah Ahmad Dahlan Cirebon.
2. Perwakilan tim melakukan peninjauan lokasi dan wawancara dengan perwakilan mitra untuk mendapatkan data lebih lanjut mengenai kondisi dan kebutuhan spesifik, serta mengonfirmasi permasalahan yang ada.



Gambar 1. Langkah Kerja

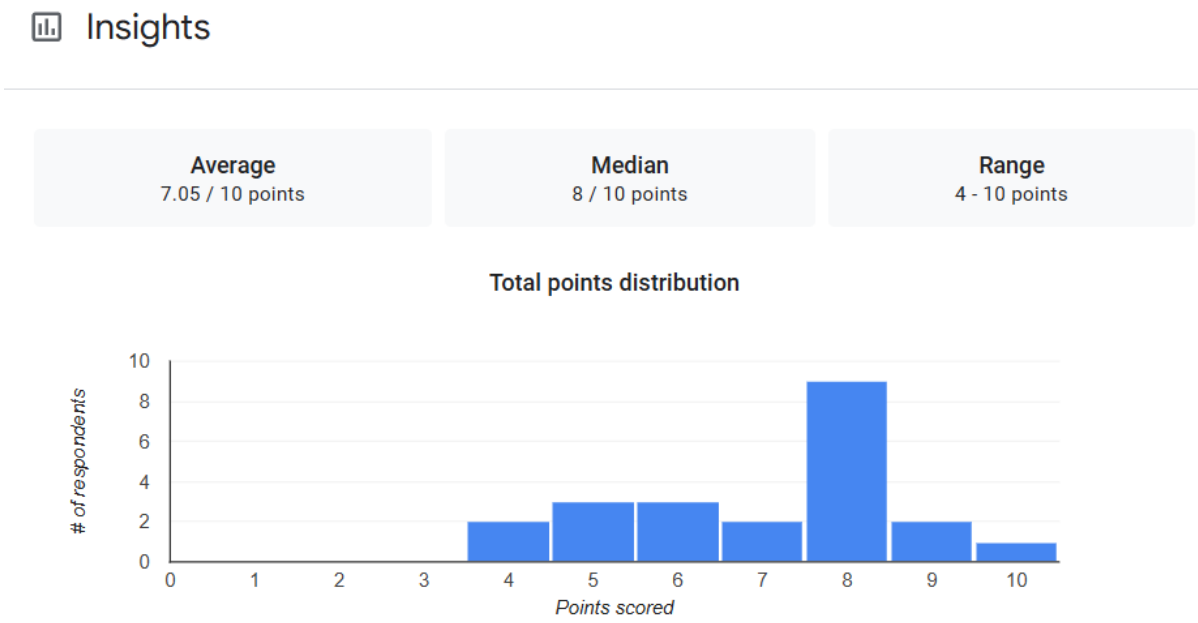
3. Proses pembuatan materi pelatihan disusun secara terstruktur, mencakup jenis serangan, dasar-dasar keamanan jaringan, pengenalan *VPN*, hingga fitur-fitur lanjutan seperti konfigurasi *L2TP, IPsec, dan WireGuard*. Materi juga disiapkan dalam bentuk presentasi *PowerPoint* agar dapat meningkatkan pemahaman (Yowenus Wenda, 2023).
4. Jadwal kegiatan disusun bersama dengan pihak mitra, termasuk penentuan durasi sesi, jumlah peserta, dan alokasi waktu untuk praktik.
5. Kegiatan dilaksanakan secara *hybrid* yang dilaksanakan pada Tanggal 11 Juli 2025 Pukul 10.00-11.30 WIB, yaitu sesi tatap muka (*offline* di kelas) dan sesi daring (*online* melalui *Zoom*). Untuk mengukur tingkat ketercapaian keberhasilan, dilakukan pre-test sebelum dan post-test setelah penyuluhan. Peran tes sebagai alat ukur berfungsi untuk mengukur perkembangan dan pertumbuhan peserta didik (Asyiah Siregar et al., n.d.). Alat ukur keberhasilan juga mencakup observasi langsung terhadap perubahan sikap dan kemampuan peserta dalam mengaplikasikan keterampilan yang diajarkan, serta pengumpulan umpan balik (*feedback*) melalui kuesioner. Media yang digunakan meliputi laptop, proyektor, materi *powerpoint*, dan contoh demo konfigurasi *VPN*.
6. Kegiatan dimonitor secara berkala untuk memastikan kelancaran dan efektivitas. Evaluasi dilakukan melalui analisis hasil pre-test dan post-test, serta umpan balik dari peserta dan mitra.

3. Hasil dan Pembahasan

Kegiatan pengabdian kepada masyarakat ini dilaksanakan di Cirebon pada. Program ini melibatkan total 20 peserta dari Civitas Akademika Universitas Muhammadiyah Ahmad Dahlan Cirebon (mahasiswa, tenaga kependidikan) dan 7 peserta dari unit IT. Pihak mitra menyambut baik rencana kegiatan ini, menunjukkan antusiasme tinggi terhadap peningkatan kapasitas digital dan keamanan jaringan mereka.

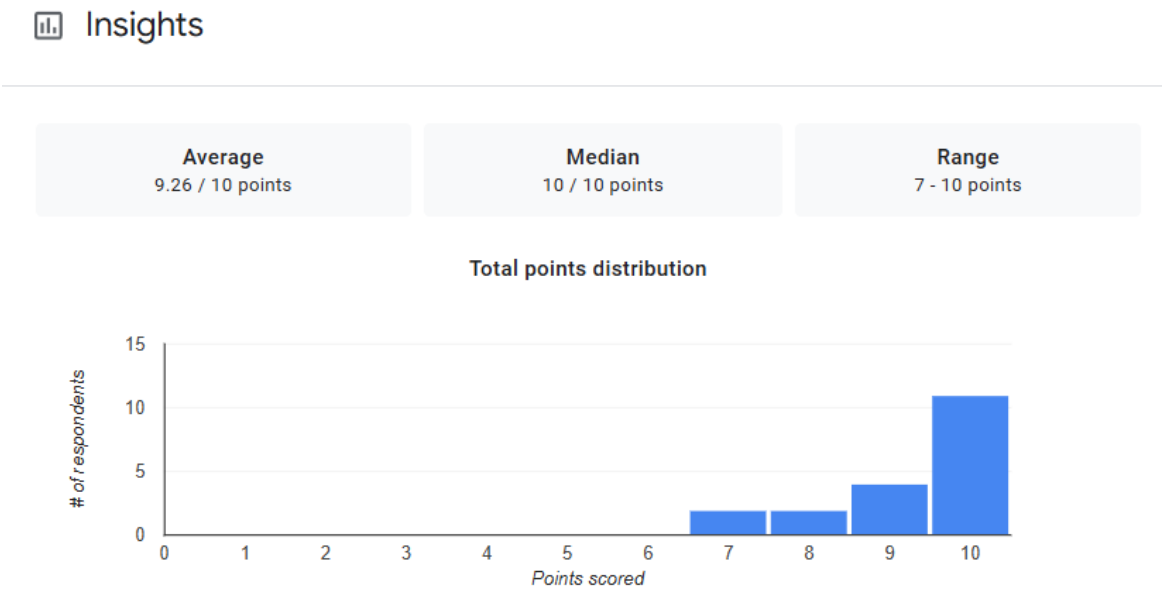
Gambar 2 Pelaksanaan Kegiatan

Pelaksanaan kegiatan difokuskan pada pelatihan interaktif yang mencakup pengenalan konsep mencakup jenis serangan, dasar-dasar keamanan jaringan, pengenalan *VPN*, hingga fitur-fitur lanjutan seperti konfigurasi *L2TP*, *IPsec*, dan *WireGuard*. Setiap sesi pelatihan dirancang dengan porsi contoh nyata memastikan peserta dapat langsung mengaplikasikan pengetahuan yang diperoleh. Indikator keberhasilan utama diukur melalui perbandingan hasil pre-test dan post-test, observasi langsung terhadap kemampuan peserta dalam menyelesaikan tugas-tugas praktis, serta pengumpulan umpan balik (*feedback*) dari peserta.



Gambar 3 Hasil Pre Test

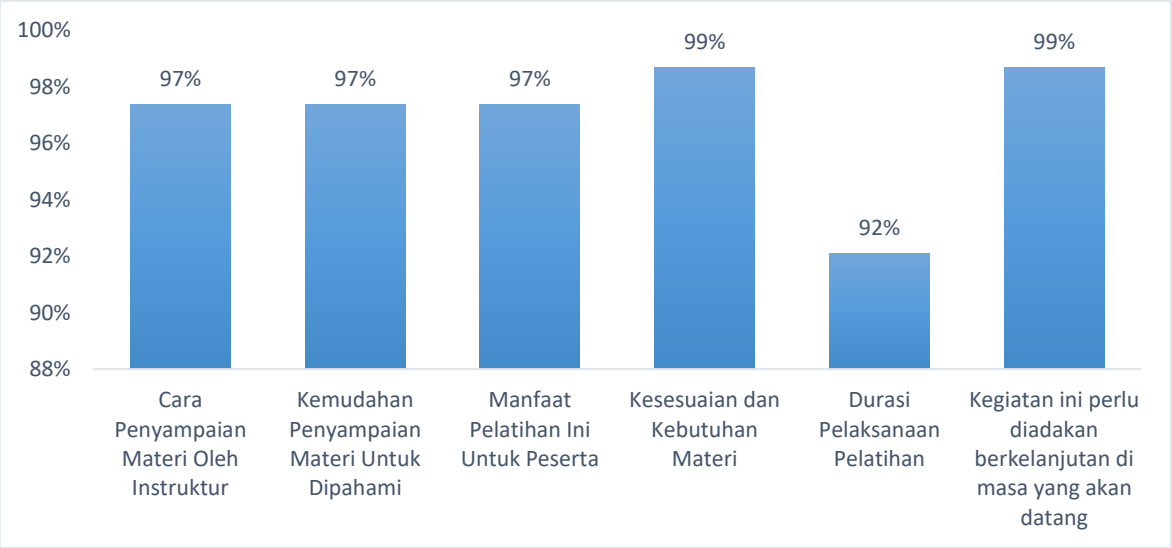
Berdasarkan Gambar 3, hasil pre-test menunjukkan gambaran awal pemahaman peserta sebelum pelatihan. Nilai rata-rata yang dicapai adalah 7,05 dari 10 poin. Nilai tengah (*median*) berada di angka 8 poin. Sementara itu, rentang nilai (*range*) yang diperoleh peserta bervariasi dari 4 hingga 10 poin. Diagram distribusi total poin memperlihatkan bahwa sebagian besar responden mendapatkan skor 8, diikuti oleh skor 5, 6, 7, 9, dan 10. Hasil ini mengindikasikan bahwa meskipun sebagian peserta sudah memiliki pemahaman awal yang cukup baik, masih ada celah pengetahuan yang perlu diisi melalui pelatihan.



Gambar 4 Hasil Post Test

Diagram distribusi total poin pada Gambar 4 menunjukkan bahwa sebagian besar responden, dengan jumlah tertinggi, berhasil mendapatkan nilai sempurna 10 poin. Skor ini jauh lebih tinggi dibandingkan dengan hasil pre-test. Peningkatan ini mengindikasikan adanya transfer pengetahuan dan peningkatan keterampilan yang efektif kepada peserta setelah program pelatihan. Hal ini menunjukkan bahwa pelatihan yang berbasis studi kasus, demo dan praktik mampu meningkatkan kesadaran siber dan memberikan dampak nyata.

Hasil yang dicapai menunjukkan peningkatan signifikan dalam pemahaman dan penguasaan konsep keamanan jaringan dan penggunaan *VPN* di kalangan peserta. Rata-rata skor post-test meningkat secara substansial dibandingkan dengan pre-test, mengindikasikan adanya transfer pengetahuan dan peningkatan keterampilan yang efektif. Umpan balik yang diterima dari peserta juga sangat positif, menyoroti relevansi materi dan metode penyampaian yang interaktif. Sebagai contoh, peserta yang sebelumnya tidak memahami cara kerja *VPN* atau perbedaan antara jenis-jenisnya, kini mampu mengidentifikasi dan mengimplementasikan solusi *VPN* yang sesuai untuk kebutuhan mereka. Hal ini memberikan nilai tambah yang nyata bagi civitas akademika, baik dalam kegiatan akademik, administrasi, maupun potensi perubahan perilaku yang lebih luas dalam memanfaatkan teknologi secara aman.



Gambar 5 Hasil *Feedback*

Secara keseluruhan, grafik pada Gambar 5 menunjukkan tingkat kepuasan dan penilaian yang sangat tinggi terhadap pelatihan tersebut. Mayoritas aspek mendapatkan persentase di atas 97%, dengan materi dan kebutuhan serta keberlanjutan kegiatan mendapatkan skor hampir sempurna (99%). Satu-satunya area dengan sedikit potensi perbaikan adalah durasi pelaksanaan pelatihan, meskipun persentasenya tetap tinggi pada 92%.

Tabel 1 Ringkasan Hasil Kegiatan dan Indikator Keberhasilan

No.	Kegiatan	Indikator Keberhasilan	Hasil yang Dicapai
1.	Pelatihan Dasar Keamanan Jaringan & VPN	Peningkatan skor pre-test ke post-test pada modul dasar keamanan jaringan	Rata-rata peningkatan skor 31.35%
2.	Pelatihan Jenis & Konfigurasi VPN (L2TP, IPsec, WireGuard)	Kemampuan mengidentifikasi dan mengkonfigurasi berbagai jenis VPN	80% peserta mampu mengkonfigurasi setidaknya satu jenis VPN
3.	Praktik Penggunaan VPN untuk Akses Aman	Kemampuan menggunakan VPN untuk akses data universitas dan komunikasi aman	75% peserta mampu mengaplikasikan VPN dalam skenario nyata
4.	Sesi Tanya Jawab & Umpan Balik	Tingkat kepuasan peserta dan relevansi materi (melalui *feedback*)	Umpan balik positif, saran untuk pelatihan lanjutan

Meskipun kegiatan berjalan lancar, beberapa tantangan dijumpai, terutama terkait dengan tingkat kemampuan awal peserta yang bervariasi dalam hal pemahaman teknis jaringan. Beberapa peserta memerlukan pendampingan lebih intensif dalam sesi praktik konfigurasi. Namun, pendekatan adaptif tim, dengan memberikan perhatian personal dan modul yang disesuaikan, berhasil mengatasi kendala ini.

4. Kesimpulan

Program pengabdian kepada masyarakat yang dilaksanakan berhasil menjawab permasalahan utama yang dihadapi Civitas Akademika Universitas Muhammadiyah Ahmad Dahlan Cirebon, yaitu rendahnya pemahaman dan praktik keamanan jaringan. Pelatihan yang diberikan mampu meningkatkan kesadaran dan keterampilan peserta secara signifikan, terbukti dari peningkatan skor post-test dan tingginya tingkat kepuasan peserta. Materi pelatihan yang aplikatif dan metode *hybrid* (tatap muka dan daring) terbukti efektif dalam menjangkau peserta

dengan latar belakang teknis yang beragam.

Program ini tidak hanya memberikan solusi sesaat, tetapi juga mendorong terbentuknya tim keamanan jaringan internal sebagai pelatih lokal, sekaligus mempersiapkan rencana pengembangan lanjutan dan publikasi hasil ke ranah ilmiah. Dengan demikian, kegiatan ini mampu memberikan kontribusi nyata dalam memperkuat budaya keamanan digital di lingkungan perguruan tinggi serta memperluas dampak literasi siber di era transformasi digital.

Referensi

Aditya, M., Ghozali, M., Witanti, W., & Abdillah, G. (2024). *JIP (Jurnal Informatika Polinema) Pengamanan Data E-Mail Menggunakan Enkripsi Partially Homomorphic Encryption (PHE)*. https://jurnal.polinema.ac.id/index.php/jip/article/view/5420

Alisalman, M. (2022). Pembelajaran Partisipatif Sebagai Metode dalam Meningkatkan Hasil Belajar Mahasiswa. *Diklus: Jurnal Pendidikan Luar Sekolah*, *6*(1), 66–77. https://doi.org/10.21831/diklus.v6i1.48572

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Dewi, S., Riyadi, F., Suwastitaratu, T., & Hikmah, N. (2020). Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis. *Jurnal Sains Dan Manajemen*, *8*(1).

Siaulhak, Syafriadi, & Alfhian Makmur. (2024). Pelatihan Keamanan dan Enkripsi Menggunakan VPN dalam Mengamankan Data. In *JAMASTIK Jurnal Abdimas Teknologi Informatika* (Vol. 2). http://jurnal.ftkom.uncp.ac.id/jamastik

Muhamad Malik Matin, I., Ramadhan, F., Hutasoit, G. S., Aurellia Hapsari, A., Teknik Informatika dan Komputer Politeknik Negeri Jakarta Jl GA Siwabessy, D. D., Beji, K., Depok, K., & Barat, J. (2024a). *Analisis Kerentanan Jaringan pada Fasilitas Internet Nirkabel pada Serangan Packet Sniffing*. *4*(1), 61–66.

Muhamad Malik Matin, I., Ramadhan, F., Hutasoit, G. S., Aurellia Hapsari, A., Teknik Informatika dan Komputer Politeknik Negeri Jakarta Jl GA Siwabessy, D. D., Beji, K., Depok, K., & Barat, J. (2024b). *Analisis Kerentanan Jaringan pada Fasilitas Internet Nirkabel pada Serangan Packet Sniffing*. *4*(1), 61–66.

Novianto, D., Japriadi, Y. S., & Tommy, L. (2022). Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard VPN Di Routerboard Mikrotik. *Jurnal Ilmiah Informatika Global*, *13*(2). https://doi.org/10.36982/jiig.v13i2.2308

Mutasar, Yustizar, Muttaqin, Rozzi Kesuma Dinata, & Novia Hasdyna. (2024). Pelatihan Dasar Jaringan Komputer bagi Pemula: Membangun Keterampilan Teknologi dari Teori ke Praktik di Kota Langsa. *Edisi Oktober-Desember*, *5*(4), 4689–4695. https://doi.org/10.55338/jpkmn.v5i4.4293

Prasetyo, S. E., Haeruddin, H., & Ariesryo, K. (2024). Website Security System from Denial of Service attacks, SQL Injection, Cross Site Scripting using Web Application Firewall. *Antivirus : Jurnal Ilmiah Teknik Informatika*, *18*(1), 27–36. https://doi.org/10.35457/antivirus.v18i1.3339

Pratama Putra, P. (2016). *SATIN-Sains dan Teknologi Informasi Pengembangan Sistem Keamanan Jaringan Menggunakan Rumusan Snort Rule (Hids) untuk Mendeteksi Serangan Nmap* (Vol. 2, Issue 1). http://jurnal.stmik-amik-riau.ac.id

Rorong, A., & Londa, Y. (2020). *Perilaku Masyarakat Di Era Digital (Studi Di Desa Watutumou Iii Kecamata Kalawat Kabupaten Minahasa Utara) Gabriella Marysca Enjel Nikijuluw*.

Sumarna, S., & Maulana, A. (2021). Implementasi Virtual Private Network Menggunakan L2TP/IPsec pada BBPK Jakarta. *EXPERT: Jurnal Manajemen Sistem Informasi Dan Teknologi*, *11*(2), 90. https://doi.org/10.36448/expert.v11i2.1829

Yowenus Wenda. (2023). *Pelatihan Pemanfaatan Powerpoint sebagai Media Pembelajaran bagi Calon Guru Praktek*. *4*, 3080–3086. https://doi.org/10.55338/jpkmn.v4i4

Widya Sari, M. (2011.). *Analisis Keamanan Jaringan Virtual Private Network (VPN) pada Sistem Online Microbanking*.