Madiun Spoor: Jurnal Pengabdian Masyarakat, Volume 6 Nomor 1 April 2026
p-ISSN 2797-1678, e-ISSN 2797-0523

PELATIHAN KEAMANAN SIBER BAGI SISWA SMK NEGERI 3 BALIKPAPAN SEBAGAI BEKAL KESIAPAN MAGANG

Agus Wijayanto[*1], Aqilah Aulya Maulidah[2], Ghina Nur Madina[3], Aljosa Maynardian[4], Azzahra Noor Istiqomah[5], Desvita Triasasa Maharani[6], Alif Rizky Saputra[7], Abiyu Dzaki[8], Dicky Pratama Candra[9], Malik Endrianove[10], Mario Sahrul Ramadhani Rahman[11], Dicky Satrio Ikhsan Utomo[12], Muhammad Fahmi Abdillah[13]

[1,2,3,4,5,6,7,8,9,10,11,12,13]Teknologi Informasi, Universitas Mulia

e-mail: [*1]aguswijayanto@universitasmulia.ac.id, [2]2312046@students.universitasmulia.ac.id, [3]2412027@students.universitasmulia.ac.id, [4]2412033@students.universitasmulia.ac.id, [5]2512055@students.universitasmulia.ac.id, [6]2512022@students.universitasmulia.ac.id, [7]2512060@students.universitasmulia.ac.id, [8]2512043@students.universitasmulia.ac.id, [9]2512010@students.universitasmulia.ac.id, [10]2512006@students.universitasmulia.ac.id, [11]2512039@students.universitasmulia.ac.id, [12]dicky@universitasmulia.ac.id, [13]fahmiabdillah@universitasmulia.ac.id

Abstrak

Kegiatan pengabdian masyarakat ini bertujuan untuk meningkatkan literasi dan kemampuan teknis siswa jurusan Teknik Komputer dan Jaringan SMK Negeri 3 Balikpapan di bidang keamanan siber. Metode yang diterapkan adalah pelatihan *hybrid* yang menggabungkan penyampaian materi konseptual dengan praktik simulasi langsung. Materi teori meliputi konsep dasar keamanan informasi, jenis-jenis ancaman siber, serta prinsip perlindungan data. Sesi praktik difokuskan pada simulasi serangan *backdoor* menggunakan lingkungan virtual dengan konfigurasi mesin penyerang Kali Linux dan mesin korban. Peserta secara aktif terlibat dalam proses instalasi, konfigurasi, dan observasi terhadap mekanisme serangan dan dampaknya. Hasil evaluasi menunjukkan pemahaman peserta mengenai kerentanan sistem dan pentingnya langkah-langkah pencegahan. Kegiatan ini juga berhasil menumbuhkan sikap kritis dan kolaboratif di antara peserta. Sebagai *output*, siswa memperoleh bekal pengetahuan praktis yang langsung relevan dengan kebutuhan dunia kerja dan persiapan magang di bidang jaringan dan sistem keamanan. Pelatihan ini membuktikan efektivitas pendekatan *learning-by-doing* dalam pendidikan vokasi teknologi informasi.

Kata kunci: *Teknik Komputer dan Jaringan; keamanan siber; simulasi serangan; pendidikan vokasi*

Abstract

This community service activity aims to improve the literacy and technical skills of students majoring in Computer and Network Engineering at SMK Negeri 3 Balikpapan in the field of cybersecurity. The method used is a hybrid training that combines conceptual material delivery with direct simulation practice. The theoretical material covers basic concepts of information security, types of cyber threats, and data protection principles. The practical sessions focused on backdoor

attack simulations using a virtual environment with Kali Linux configured as both the attacker and victim machines. Participants were actively involved in the installation, configuration, and observation of attack mechanisms and their impacts. The evaluation results showed a significant improvement in participants' understanding of system vulnerabilities and the importance of preventive measures. This activity also succeeded in fostering a critical and collaborative attitude among participants. As a result, students gained practical knowledge directly relevant to the needs of the workforce and internship preparation in the field of network and security systems. This training proves the effectiveness of the learning-by-doing approach in information technology vocational education.

Keywords: Computer and Network Engineering; cybersecurity; attack simulation; vocational education

PENDAHULUAN

Literasi keamanan siber kini menjadi fondasi esensial dalam mempersiapkan individu menghadapi tantangan dan risiko yang melekat pada interaksi digital (Yudistira et al., 2025). Hal ini diperkuat oleh fakta bahwa minimnya pemahaman mengenai pentingnya menjaga data pribadi dan cara menghadapi berbagai ancaman digital seringkali menjadi celah eksploitasi (Wijayanto, 2024). Misalnya, ancaman seperti phishing, peretasan akun, dan penyalahgunaan data pribadi semakin marak terjadi akibat rendahnya kesadaran dan pengetahuan digital di kalangan masyarakat (Revilia & Irwansyah, 2020). Data pribadi, khususnya, menjadi aset krusial yang tidak boleh disebarluaskan secara sembarangan guna mencegah tindak kejahatan siber.

Selain itu, meningkatnya ketergantungan pada teknologi digital dalam sektor pendidikan, yang melibatkan penyimpanan dan pemrosesan data sensitif siswa dan guru pada platform daring, semakin mempertegas urgensi literasi keamanan siber untuk melindungi dari pelanggaran data (Ardhana et al., 2024). Oleh karena itu, integrasi edukasi keamanan siber dalam kurikulum pendidikan vokasi menjadi krusial untuk membekali calon tenaga teknis dengan pemahaman yang komprehensif mengenai perlindungan data dan mitigasi risiko siber (Syaddam, 2024). Kesadaran akan prinsip-prinsip dasar keamanan siber, termasuk penggunaan kata sandi yang kuat, enkripsi data, dan pembaruan sistem secara rutin, sangat penting untuk mencegah insiden keamanan (Wijayanto et al., 2025). Kemampuan untuk mengidentifikasi dan merespons upaya kejahatan digital, seperti pencurian identitas atau penyalahgunaan data, juga merupakan komponen integral dari literasi digital yang efektif (Prakasa, 2020).

Siswa Sekolah Menengah Kejuruan (SMK), khususnya jurusan Teknik Komputer dan Jaringan (TKJ), dipersiapkan untuk langsung terjun ke dunia kerja sebagai tenaga terampil tingkat menengah (Prayitno et al., 2024). Kurikulum yang diterapkan umumnya menekankan pada kemampuan teknis instalasi jaringan, konfigurasi perangkat, dan pemeliharaan sistem (Idris et al., 2025; Tengah et al., 2022). Namun, aspek keamanan siber seringkali belum terintegrasi secara komprehensif dan praktis dalam pembelajaran. Padahal, lulusan TKJ akan banyak berhadapan dengan infrastruktur jaringan yang rentan terhadap berbagai bentuk serangan, mulai dari malware, phising, hingga eksploitasi celah keamanan (Tandirerung et al., 2023). Kesenjangan antara kompetensi teknis yang diajarkan dengan tuntutan keamanan di dunia kerja nyata dapat mengurangi daya saing dan kesiapan lulusan SMK.

Mitra dalam kegiatan pengabdian ini, yaitu SMK Negeri 3 Balikpapan, mengidentifikasi kebutuhan mendesak untuk memperkuat kompetensi keamanan siber siswanya. Kebutuhan ini

muncul dari masukan dunia industri mitra sekolah dan observasi terhadap tantangan yang dihadapi alumni selama magang maupun bekerja (Endra et al., 2024). Siswa seringkali memahami teori jaringan namun kurang siap menghadapi skenario nyata terkait pelanggaran keamanan data atau serangan terhadap sistem yang mereka kelola (Afiansyah et al., 2022). Oleh karena itu, diperlukan intervensi pembelajaran yang tidak hanya bersifat teoritis tetapi juga memberikan pengalaman langsung (*hands-on experience*) dalam lingkungan yang terkendali dan aman (Marwati et al., 2025).

Berdasarkan latar belakang tersebut, kegiatan pengabdian masyarakat ini dirancang dengan tujuan: (1) meningkatkan kesadaran dan pemahaman siswa TKJ SMK Negeri 3 Balikpapan mengenai pentingnya keamanan informasi dan berbagai bentuk ancaman siber kontemporer; (2) memberikan pelatihan praktis melalui simulasi serangan siber dasar menggunakan perangkat lunak virtualisasi untuk mengilustrasikan mekanisme serangan dan dampaknya; serta (3) membekali siswa dengan pengetahuan prosedural untuk melakukan pencegahan dan mitigasi awal terhadap ancaman keamanan siber. Diharapkan, melalui kegiatan ini, siswa tidak hanya menjadi pengguna teknologi yang pasif, tetapi juga menjadi praktisi yang kritis dan responsif terhadap isu keamanan digital, sehingga meningkatkan nilai tambah kompetensi mereka menuju kesiapan magang dan dunia kerja.

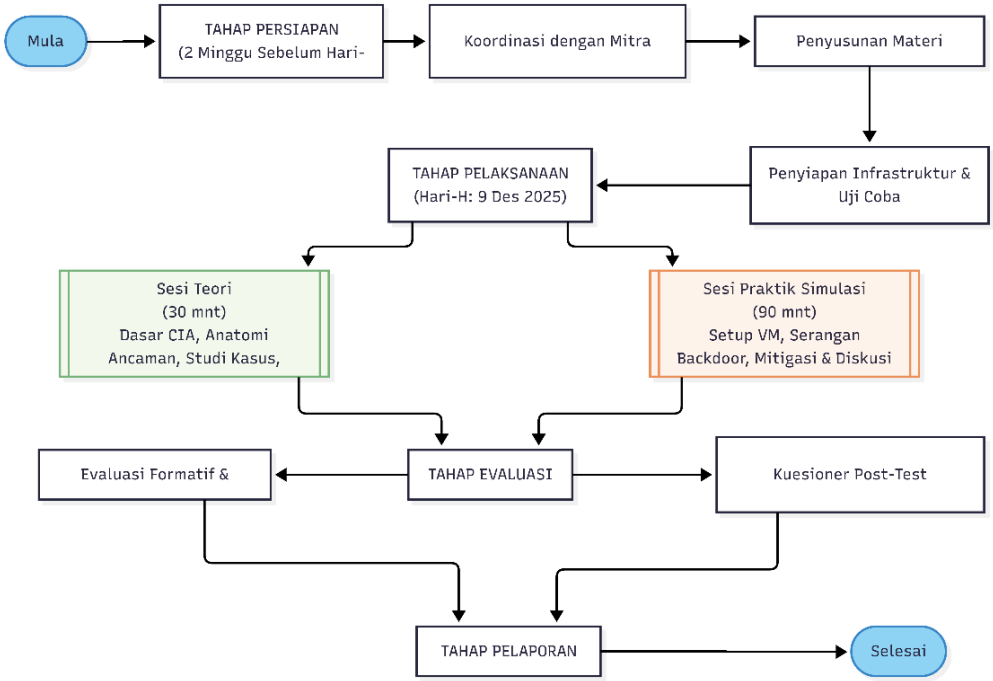
Pendekatan pelatihan partisipatif dan eksperiensial yang diadopsi dalam kegiatan ini mengacu pada *Experiential Learning Theory* yang dikemukakan oleh Kolb (Jurnal et al., 2025), yang menekankan bahwa pembelajaran efektif terjadi melalui siklus pengalaman, refleksi observasi, konseptualisasi, dan eksperimentasi aktif. Dalam konteks pendidikan vokasi, pendekatan ini memungkinkan siswa tidak hanya memahami konsep keamanan siber secara teoretis, tetapi juga mengalami langsung dinamika serangan dan pertahanan dalam lingkungan yang terkendali.

Secara metodologis, kegiatan ini mengadopsi pendekatan pelatihan partisipatif dan eksperiensial (Purwawijaya et al., 2025). Kajian pustaka yang mendasari meliputi konsep information security awareness, kerangka ethical hacking untuk pendidikan, serta efektivitas pembelajaran berbasis simulasi dalam pendidikan vokasi teknik. Dengan menggabungkan teori dan praktik dalam satu paket pelatihan intensif, kegiatan ini diharapkan dapat menjembatani kesenjangan antara kurikulum sekolah dan dinamika keamanan siber di industri.

Program pengabdian ini berbeda dengan program pelatihan keamanan siber serupa di SMK lainnya adalah fokus pada simulasi serangan *backdoor* yang jarang dipraktikkan secara langsung di lingkungan sekolah karena keterbatasan infrastruktur dan kekhawatiran risiko keamanan. Dengan memanfaatkan lingkungan virtual terisolasi, peserta dapat mengeksplorasi mekanisme serangan dan dampaknya tanpa membahayakan jaringan sekolah atau perangkat pribadi. Selain itu, penyelarasan materi dengan kebutuhan magang menjadi nilai tambah utama, di mana simulasi dirancang berdasarkan masukan dari industri mitra sekolah mengenai kompetensi keamanan siber yang diharapkan dari lulusan TKJ. Pendekatan ini tidak hanya meningkatkan literasi teknis siswa, tetapi juga membentuk sikap kritis dan responsif terhadap ancaman digital yang relevan dengan dunia kerja.

METODE PELAKSANAAN

Kegiatan pengabdian masyarakat ini dilaksanakan dengan menerapkan metode pelatihan partisipatif dan eksperiensial, yang dirancang untuk memastikan peserta tidak hanya memahami konsep teori tetapi juga memperoleh pengalaman langsung melalui simulasi praktik. Pelaksanaan dilakukan secara terstruktur melalui beberapa tahapan utama, sebagaimana ditampilkan dalam Gambar 1.



Gambar 1. Alur pelaksanaan kegiatan pengabdian

Diagram alir yang ditunjukkan pada gambar 1dikelompokkan kepada tiga bagian utama sebagai berikut:

1. Tahap Persiapan; Tahap persiapan dilakukan selama dua minggu sebelum hari pelaksanaan. Langkah-langkahnya meliputi:
   a. Koordinasi dengan Mitra: Tim pengabdi melakukan pertemuan dengan pihak SMK Negeri 3 Balikpapan, yang diwakili oleh koordinator jurusan TKJ, untuk melakukan diskusi, menyepakati waktu, tempat, sasaran peserta (dua kelas TKJ), dan kebutuhan teknis. Selain itu dalam sesi diskusi, data yang dibutuhkan untuk menunjang persiapan pelaksanaan pelatihan diantaranya kurikulum yang diajarkan dan kompetensi siswa berdasarkan evaluasi kordinator TKJ,
   b. Penyusunan Materi dan Modul: Materi pelatihan disusun berdasarkan analisis kebutuhan dan kurikulum dasar keamanan siber. Modul dibagi menjadi dua bagian utama: (a) Buku Panduan Teori yang mencakup pengantar keamanan siber, jenis ancaman, dan prinsip pertahanan; dan (b) Petunjuk Praktikum simulasi serangan *backdoor* menggunakan VirtualBox, Kali Linux, dan Windows 7. Untuk memastikan pembelajaran ini aman, semua dilakukan pada jaringan yang terisolasi dengan memanfaatkan *tools virtualbox.* Hal ini mencegah virus untuk terhubung ke jaringan nyata dilokasi pelatihan.
   c. Penyiapan Infrastruktur: Tim melakukan pengecekan dan penyiapan perangkat lunak yang diperlukan (software image Kali Linux dan Windows 7, VirtualBox)
2. Tahap Pelaksanaan; Kegiatan utama dilaksanakan pada Selasa, 9 Desember 2025, di kelas SMK Negeri 3 Balikpapan, yang terbagi menjadi dua sesi paralel (Sesi I untuk TKJ 1 dan Sesi II untuk TKJ 2). Struktur pelaksanaan setiap sesi adalah sebagai berikut:
   a. Pembukaan dan Pengantar: Dipandu oleh MC, berisi sambutan, penyampaian tujuan, dan gambaran umum agenda pelatihan.

b. Sesi Teori – Sosialisasi Konsep Keamanan Siber (60 menit termasuk *pre-test* dan *post-test*): Pemateri menyampaikan materi secara interaktif dengan presentasi multimedia. Cakupan materi meliputi: Konsep dasar Confidentiality, Integrity, Availability (CIA Triad); ancaman siber umum seperti *Malware, Phishing, Social Engineering, DDoS*; Prinsip dasar pengamanan diri dan system.
c. Sesi Praktik (60 menit) – Simulasi Serangan Siber

3. Tahap Evaluasi dan Pelaporan: evaluasi dilakukan secara formatif selama proses dan sumatif di akhir kegiatan. Dalam pelaksaan evaluasi, tim pengabdi menggunakan fasilitas *google form* dengan membuat kuis serta observasi langsung guna melihat kemampuan mengikuti langkah simulasi, ketepatan konfigurasi.

Metode pelaksanaan yang sistematis ini memastikan kegiatan berjalan terarah, partisipatif, dan mencapai tujuan yang telah ditetapkan, yaitu memberikan pengalaman belajar langsung yang berdampak pada peningkatan kompetensi peserta.

PEMBAHASAN

1. Keterlibatan dan Pencapaian Pembelajaran Peserta

Kegiatan pengabdian masyarakat yang dilaksanakan di SMK Negeri 3 Balikpapan berhasil mencapai tujuan yang telah ditetapkan. Pembahasan berikut menguraikan hasil analisis terhadap pelaksanaan kegiatan, yang mencakup aspek partisipasi, pencapaian pembelajaran, dampak, serta kendala dan solusi yang ditemui. Data dan observasi yang disajikan merujuk pada proses selama sesi teori dan praktik, serta hasil evaluasi dari peserta. Tingkat kehadiran peserta mencapai 100% dari total undangan yang meliputi dua kelas TKJ. Selama sesi berlangsung, antusiasme peserta terlihat tinggi, khususnya pada saat sesi praktik simulasi keamanan siber. Interaksi selama sesi tanya jawab menunjukkan bahwa peserta tidak hanya pasif menerima materi, tetapi aktif mengajukan pertanyaan terkait kasus keamanan siber yang pernah mereka dengar atau alami secara tidak langsung, seperti kasus penipuan phishing melalui media sosial. Hal ini mengindikasikan bahwa materi yang disampaikan relevan dengan konteks pengalaman digital mereka sehari-hari.

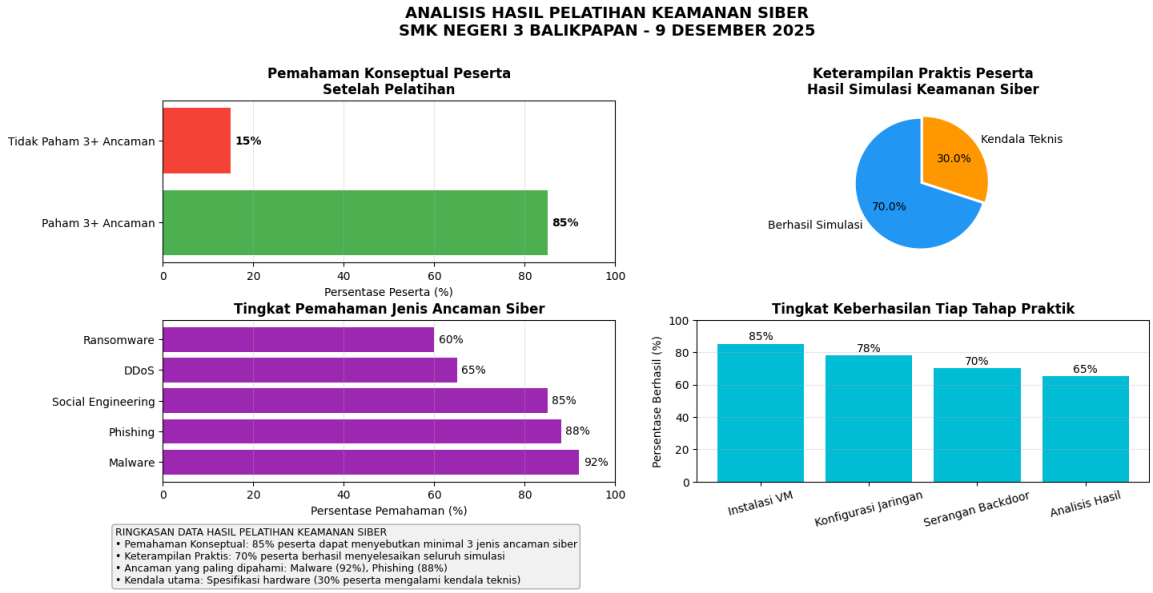
(a)

(b)

Gambar 2. (a) Pemaparan materi dan (b) pendampingan dari setiap mahasiswa ke peserta pelatihan.

Berdasarkan hasil observasi dan kuesioner *post-test* setelah pelaksanaan palatihan, terjadi peningkatan pemahaman peserta dalam beberapa aspek kunci, namun kekurangan evaluasi tidak membandingkan uji statistik:

a) Pemahaman Konseptual: Sebelum pelatihan, sebagian besar peserta hanya mengenal istilah "*hacker*" dalam konteks negatif tanpa memahami metode serangannya. Setelah sesi teori, 85% peserta (berdasarkan sampling respons), di mana ini bagian dari observasi langsung dengan melempar pertanyaan dilakukan secara acak perkelas ini dapat menyebutkan minimal tiga jenis ancaman siber (*malware*, *phishing*, dan *social engineering*) dan menjelaskan prinsip dasar pencegahan. Per-kelas dilakukan pertanyaan untuk lima siswa dengan empat diantaranya mampu langsung menjelaskan.
b) Keterampilan Praktis: Pada sesi praktik, sekitar 70% peserta berhasil menyelesaikan seluruh tahap simulasi, mulai dari instalasi virtual machine, konfigurasi jaringan antara Kali Linux dan Windows 7, hingga menjalankan dan mengamati serangan *backdoor*. Data ini akumulasi dari penilaian instalasi *virtual machine*, mengkonfigurasi jaringan yang terisolasi, membuat malware dan menanamkan *backdoor* dan observasi dampak setelah uji serangan dilakukan. Peserta yang mengalami kendala teknis (30%) terutama terkait spesifikasi *hardware* komputer yang kurang memadai, Penggunaan *virtual machine* terutama untuk kali linux cukup memakan banyak sumber daya memori, Ketika perangkat terbatas dengan hanya memiliki spesifikasi memori 4GB ini akan memperlambat kinerja hingga terkadang bisa menyebabkan system utama berhenti. Dalam praktik ini dua sistem operasi dijalankan di *virtual machine* sehingga beban memori yang harus dialokasikan setidaknya 8 GB. Namun tetap dapat mengikuti melalui bimbingan langsung dari tim pendamping dan kerja sama dengan peserta lain. Kolaborasi ini menciptakan lingkungan belajar yang saling mendukung (*peer-assisted learning*). Data ditampilkan dalam bentuk gambar 3.



Gambar 3. Visualisasi data evaluasi peserta

2. Relevansi Kegiatan dengan Kebutuhan Magang dan Dunia Kerja

   Salah satu fokus kegiatan adalah menyelaraskan materi dengan kompetensi yang dibutuhkan dalam dunia kerja, khususnya persiapan magang. Dari diskusi dengan perwakilan guru TKJ, diketahui bahwa industri mitra sekolah seringkali mengharapkan lulusan SMK yang tidak hanya mampu mengkonfigurasi jaringan, tetapi juga memiliki kesadaran keamanan dasar. Simulasi yang dilakukan memberikan gambaran nyata tentang kerentanan sistem yang tidak terupdate dan kurang terproteksi, yang sering dijumpai di lapangan. Dengan demikian, peserta mendapatkan *awareness* praktis yang langsung dapat diterapkan, misalnya dalam menjaga keamanan jaringan lokal selama praktik kerja lapangan atau magang.
3. Analisis Kendala

   Pelaksanaan kegiatan dihadapkan pada beberapa kendala teknis dan non-teknis, beserta solusi yang diambil:

   a) spesifikasi laptop menjadi hal utama menyebabkan beberapa unit lambat saat menjalankan dua *virtual machine* secara bersamaan;
   b) perbedaan kecepatan pemahaman peserta menyebabkan sebagian merasa tertinggal pada tahap konfigurasi jaringan; dan
   c) waktu pelatihan yang terbatas.

   Beberapa kendala yang kemudian dialami beberapa bisa diatasi, mulai dari sharing laptop untuk menunjukkan hasil serangan yang dipraktikan, terkait dengan kecepatan pemahaman membagi peserta ke dalam kelompok kecil yang dipandu oleh satu anggota tim HIMATI, memastikan semua kelompok tetap pada fase yang sama.
4. Dampak terhadap Motivasi dan Rencana Tindak Lanjut

   Di akhir sesi, banyak peserta yang menyatakan ketertarikan untuk mendalami keamanan siber secara mandiri. Beberapa peserta bahkan meminta rekomendasi sumber belajar *online* dan *platform* latihan (*cyber range*) untuk berlatih secara legal. Respon positif ini menjadi indikator bahwa kegiatan berhasil memicu motivasi intrinsik peserta. Sebagai tindak lanjut, pihak sekolah

berencana mengintegrasikan modul pelatihan singkat ini ke dalam kegiatan ekstrakurikuler atau *bootcamp* khusus TKJ, dengan dukungan materi dari tim pengabdi.

(a) (b)

Gambar 4. Foto bersama diakhir sesi (a) kelas A dan (b) kelas B

Secara keseluruhan, kegiatan pengabdian ini membuktikan bahwa pendekatan pembelajaran berbasis simulasi dan langsung praktik (*hands-on simulation*) sangat efektif untuk meningkatkan kompetensi keamanan siber siswa vokasi. Hasilnya tidak hanya terukur dari peningkatan pengetahuan, tetapi juga dari terbentuknya sikap kritis, kolaboratif, dan kesadaran akan tanggung jawab sebagai calon profesional di bidang teknologi informasi.

KESIMPULAN

Berdasarkan keseluruhan pelaksanaan kegiatan, dapat disimpulkan bahwa pelatihan keamanan siber ini berhasil mencapai tujuan yang ditetapkan. Kegiatan ini secara efektif meningkatkan pemahaman konseptual peserta mengenai ancaman siber, di mana 85% peserta mampu mengidentifikasi minimal tiga jenis ancaman siber beserta mekanisme pencegahannya setelah mengikuti sesi teori. Pada aspek keterampilan praktis, sebanyak 70% peserta berhasil menyelesaikan seluruh tahapan simulasi keamanan siber, meliputi instalasi *virtual machine*, konfigurasi jaringan, dan eksekusi serangan *backdoor* dalam lingkungan terkendali. Kendala teknis yang dialami sebagian peserta justru menjadi momentum pembelajaran kolaboratif melalui pendampingan teman sebaya dan tim fasilitator. Hasil ini menunjukkan bahwa pendekatan pembelajaran berbasis simulasi dan praktik langsung relevan dengan kebutuhan pengembangan kompetensi siswa SMK jurusan TKJ, khususnya dalam mempersiapkan mereka menghadapi tantangan dunia kerja dan magang di bidang teknologi informasi. Keberhasilan kegiatan ini juga membuka peluang pengembangan program berkelanjutan dan integrasi materi keamanan siber ke dalam kurikulum tambahan maupun ekstrakurikuler di sekolah mitra. Adapun saran untuk kegiatan selanjutnya mengingat beberapa keandala diamali maka perlu Penyediaan laboratorium virtual (*cyber lab*) yang dapat diakses secara *online* untuk latihan mandiri, Pengembangan modul pelatihan dengan tingkat kesulitan berjenjang (*beginner to intermediate*) dan Pelatihan lanjutan khusus untuk siswa yang memiliki minat mendalam di bidang *cybersecurity*. Secara keseluruhan, kegiatan ini telah mencapai tujuan yang ditetapkan dan memberikan kontribusi nyata dalam meningkatkan kompetensi serta kesiapan siswa SMK Negeri 3 Balikpapan menghadapi tantangan keamanan siber di era digital.

DAFTAR PUSTAKA

Afiansyah, H. G., Annisa, N., & Febriyani, K. (2022). Penyusunan Kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST. *Jurnal Info Kripto*, *17*(1).

Ardhana, V. Y. P., Sugiarto, Putra, Y. W. S., Handayani, R. D., Djumhadi, Mulyodiputro, D., Kusuma, A. F. A. A., Agus Wijayanto, S.Kom., M. K., Fatkhurrochman, Kumoro, D. T., Dwi Astuti, S. K., Priyoatmoko, W., Hafidudin, & Dodi Setiawan. (2024). *Konsep Dasar Teknologi Informasi* (Sugiarto & V. Y. P. Ardhana (eds.); 1st ed., Issue 112). CV. Mega Press Nusantara. https://megapress.co.id/product/konsep-dasar-teknologi-informasi/

Endra, R. Y., Redaputri, A. P., Dunan, H., Kurniawan, A., Komputer, F. I., Lampung, U. B., Lampung, U. B., Hukum, F., Lampung, U. B., & Sebesi, P. (2024). PELATIHAN PRAKTIS : MENGUASAI MICROSOFT OFFICE DENGAN MUDAH DI SDN TEJANG PULAU SEBESI KALIANDA LAMPUNG. *Madiun Spoor : Jurnal Pengabdian Masyarakat*, *4*(1), 34–40. https://doi.org/https://doi.org/10.37367/jpm.v4i1.341

Idris, N. Bin, Wijayanto, A., Servanda, Y., & Aditya, P. (2025). *PELATIHAN GURU SMK TKJ DALAM MENGGUNAKAN CISCO PACKET*. *4*(1), 191–196. https://doi.org/10.47002/jpm.v4i1.877

Jurnal, M., Cahyaningrum, D., Wayan, N., Mutiara, A., Dewi, I., Ibrahim, K., Manajemen, S., Ekonomi, F., & Mataram, U. (2025). *Penguatan Kolaborasi Guru SMK melalui Outbound Training : Perspektif Experiential Learning*. *4*(4), 348–361. https://doi.org/10.54259/manabis.v4i4.5844

Marwati, F., Astofa, A., Studi, P., Informasi, S., Pamulang, U., & Security, D. (2025). *Pelatihan Cyber Security Sebagai Pengetahuan Dasar Keamanan Untuk Peningkatan Security Awarness*. *3*.

Prakasa, J. E. W. (2020). Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi. *Jurnal Ilmiah Teknologi Informasi Asia*, *14*(2), 75. https://doi.org/10.32815/jitika.v14i2.452

Prayitno, P. P. I., Bin Idris, N., Prayogo, M. A., Sudinugraha, T., Wijayanto, A., Dwiatma, Y., & Vidy, V. (2024). PELATIHAN PENGEMBANGAN KETERAMPILAN SISWA DENGAN MENERAPKAN TEKNOLOGI DALAM PENDIDIKAN. *JURNAL MULIA*, *3*(1), 129–133. https://doi.org/10.47002/jpm.v3i1.782

Purwawijaya, E., Syahputra, D., Singarimbun, R. N., & Rambe, A. (2025). *Pelatihan Kesadaran Keamanan Informasi bagi Karyawan PT . Wijaya Kesuma Segara untuk Mencegah Ancaman Siber*. *2*(1), 50–55.

Revilia, D., & Irwansyah, N. (2020). Social Media Literacy: Millenial's Perspective of Security and Privacy Awareness. *Jurnal Penelitian Komunikasi Dan Opini Publik*, *24*(1), 478416

Syaddam. (2024). *Sosialisasi Keamanan Data di Dunia Siber untuk Meningkatkan Kewaspadaan SMK 1 Negeri Tarakan Terhadap Ancaman Cybercrime*. *3*(2), 289–299.

Tandirerung, V. A., Riana T. Mangesa, & Syahrul. (2023). Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas. *TEKNOVOKASI : Jurnal Pengabdian Masyarakat*, *1*(2), 89–94. https://doi.org/10.59562/teknovokasi.v1i2.131

Tengah, L., Yadnya, M. S., Budiman, D., Ramadhani, C., Kanata, B., Sudi, P., Elektro, J. T., Teknik, F., & Mataram, U. (2022). PROGRAM PENINGKATAN DAN PELATIHAN KURIKULUM TEKNOLOGI KOMPUTER JARINGAN TINGKAT SMK TERPADU YAYASAN GEMA

CENDEKIA MUSLIM LOMBOK TENGAH. *JURNAL ABDI INSANI*, *9*, 1374–1379

Wijayanto, A. (2024). Mengenal Cybersecurity: Perlindungan Data Pribadi Dan Privasi Di Sma Negeri 1 Samboja. *Jurnal Mulia*, *3*(2), 165–172. https://doi.org/10.47002/jpm.v3i2.867

Wijayanto, A., Abdillah, M. F., Maulidah, A. A., Maynardian, A., Madina, G. N., Wijaya, A., Gerungan, R. A. C., Najha, N., Ahsani, A. Z., Ramadhan, S. M., Triwahyudi, R. D., & Zistafa, E. R. (2025). Peningkatan Kesadaran Keamanan Siber Siswa SMK Melalui Pelatihan Dan Simulasi Serangan Dalam Lingkungan Virtual. *BERBAKTI: Jurnal Pengabdian Kepada Masyarakat*, *3*(3), 278–285. https://doi.org/https://doi.org/10.30822/hj4rr981

Yudistira, N., Lamba, E. F., Jauhari, R., Farhanna, F. R., & Yayu'Palangan, C. (2025). Penyuluhan Keamanan Informasi Terkait Ancaman Phishing untuk Meningkatkan Literasi Digital Warga Kompleks Yadara Babarsari Yogyakarta. *GIAT: Teknologi Untuk Masyarakat*, *4*(1), 52–63