

Think Like a Hacker, Act Like a Defender: Pelatihan Ethical Hacking bagi Siswa SMA Kristen Karunia Jakarta

Muhammad Adrinta Abdurrazzaq^{1)*}, Edwin Lesmana Tjiong²⁾, Harya Bima Dirgantara³⁾,
Atha Fa'iq Abdurrochman⁴⁾, Aqil Ihsaan⁵⁾

^{1,2,3,4,5)} Informatika, Fakultas Ilmu Komputer dan Desain, Universitas Kalbis, Jl. Pulomas Selatan Kav. No.22,
RT.6/RW.9, Kayu Putih, Kec. Pulo Gadung, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta 13210

*Email Korespondensi: muhammad.abdurrazzaq@kalbis.ac.id

Email: edwin.tjiong@kalbis.ac.id

Email: harya.dirgantara@kalbis.ac.id

Email: 2024105659@student.kalbis.ac.id

Email: 2024105623@student.kalbis.ac.id

Abstract: *The rapid advancement of digital transformation has increased the complexity of cyber threats, creating a growing need for enhanced digital security literacy, particularly among younger generations. High school students, as digital natives, need to be equipped with cybersecurity knowledge to protect personal data and use technology responsibly. This training program aims to introduce the fundamental concepts of Ethical Hacking as an approach to understanding how cyberattacks operate in order to build stronger defense systems, rather than engaging in illegal hacking activities. The training materials cover the principles of Ethical Hacking, system vulnerability identification, information-gathering techniques, and mitigation strategies against potential cyber threats. Through an educational and practice-based approach, participants are encouraged to develop critical thinking, attention to detail, and ethical awareness in addressing digital security challenges. The expected outcomes include increased cybersecurity awareness, improved ability to identify digital risks, and the development of students who can become responsible, ethical, and security-conscious users and future developers of technology.*

Keywords: *Ethical Hacking, cybersecurity awareness, information security, cybersecurity literacy, digital generation.*

Abstrak: Transformasi digital yang semakin pesat telah meningkatkan kompleksitas ancaman siber, sehingga menuntut peningkatan literasi keamanan digital, khususnya di kalangan generasi muda. Siswa SMA sebagai digital native perlu dibekali pemahaman mengenai keamanan siber agar mampu melindungi data pribadi dan menggunakan teknologi secara bertanggung jawab. Kegiatan pelatihan ini bertujuan memperkenalkan konsep dasar *Ethical Hacking* sebagai pendekatan untuk memahami cara kerja serangan siber dalam rangka membangun sistem pertahanan yang lebih kuat, bukan untuk melakukan tindakan peretasan ilegal. Materi pelatihan meliputi pengenalan prinsip-prinsip *Ethical Hacking*, identifikasi kerentanan sistem, teknik pengumpulan informasi, serta strategi mitigasi terhadap potensi serangan siber. Melalui pendekatan edukatif dan berbasis praktik, peserta didorong untuk mengembangkan pola pikir kritis, teliti, dan beretika dalam menghadapi tantangan keamanan digital. Hasil yang diharapkan adalah meningkatnya kesadaran keamanan siber, kemampuan mengenali risiko digital, serta terbentuknya karakter siswa yang mampu menjadi pengguna sekaligus pengembang teknologi yang aman, bertanggung jawab, dan berintegritas di masa depan.

Kata kunci: *Ethical Hacking, cybersecurity awareness, keamanan informasi, literasi keamanan siber, generasi digital.*

I. PENDAHULUAN

Perkembangan teknologi digital telah mengubah hampir seluruh aspek kehidupan, mulai dari komunikasi, pendidikan, hingga

aktivitas ekonomi. Di balik berbagai kemudahan tersebut, risiko keamanan siber juga mengalami peningkatan yang signifikan. Serangan seperti *phishing*, pencurian

identitas, kebocoran data, dan penyalahgunaan akun digital semakin sering terjadi, sehingga literasi keamanan siber menjadi kompetensi yang penting dimiliki oleh masyarakat, khususnya generasi muda. Indeks Masyarakat Digital Indonesia (IMDI) 2025 menunjukkan bahwa peningkatan pemanfaatan teknologi digital perlu diimbangi dengan penguatan aspek keamanan digital agar masyarakat mampu beraktivitas secara aman dan bertanggung jawab.

Siswa SMA merupakan kelompok yang sangat aktif memanfaatkan internet dan berbagai platform digital dalam kegiatan belajar maupun kehidupan sehari-hari. Namun, tingginya intensitas penggunaan teknologi belum selalu diikuti dengan pemahaman yang memadai mengenai ancaman siber dan cara mitigasinya. Kondisi ini berpotensi meningkatkan risiko menjadi korban kejahatan siber maupun melakukan tindakan yang tidak sesuai dengan etika digital akibat kurangnya pemahaman. Oleh karena itu, pendidikan keamanan siber perlu diperkenalkan sejak dini melalui pendekatan yang mudah dipahami, aplikatif, dan berorientasi pada pembentukan karakter.

Salah satu pendekatan yang relevan adalah pengenalan *Ethical Hacking*, yaitu praktik mengidentifikasi dan mengevaluasi kerentanan sistem secara legal dan etis untuk meningkatkan keamanan informasi. Pembelajaran *Ethical Hacking* tidak berfokus pada aktivitas peretasan ilegal, melainkan pada pengembangan kemampuan berpikir analitis, pemecahan masalah, serta tanggung jawab profesional dalam melindungi sistem informasi. Melalui pelatihan ini, siswa/i SMA Kristen Karunia Jakarta diharapkan memperoleh pemahaman dasar mengenai konsep keamanan siber, identifikasi kerentanan, serta langkah-langkah mitigasi sederhana. Kegiatan ini juga bertujuan menumbuhkan kesadaran akan pentingnya etika digital sehingga peserta mampu menjadi pengguna teknologi yang cerdas, bertanggung jawab, serta berkontribusi dalam menciptakan ekosistem digital yang aman.

II. METODE PELAKSANAAN

Kegiatan pengabdian kepada masyarakat dilaksanakan secara tatap muka di SMA Kristen Karunia Jakarta sebagai mitra tunggal. Metode yang digunakan meliputi penyampaian materi, diskusi interaktif, demonstrasi sederhana, dan sesi tanya jawab mengenai konsep dasar *Ethical Hacking*. Materi difokuskan pada pengenalan pola pikir *ethical hacker*, identifikasi kerentanan sistem, pentingnya etika dalam keamanan siber, serta langkah-langkah mitigasi terhadap ancaman digital. Peserta didorong untuk menganalisis berbagai kasus sederhana sehingga mampu memahami potensi risiko dan solusi yang tepat. Melalui pendekatan edukatif dan partisipatif, kegiatan ini bertujuan meningkatkan literasi keamanan siber, membangun kesadaran akan pentingnya perlindungan data, serta menumbuhkan sikap bertanggung jawab dalam pemanfaatan teknologi digital.

III. HASIL DAN PEMBAHASAN

A. Pelaksanaan Kegiatan Pelatihan

Kegiatan pengabdian kepada masyarakat dilaksanakan di SMA Kristen Karunia Jakarta melalui metode ceramah, diskusi interaktif, demonstrasi, dan tanya jawab. Materi yang disampaikan meliputi pengenalan konsep *Ethical Hacking*, ancaman keamanan siber, identifikasi kerentanan sistem, serta pentingnya etika dalam pemanfaatan teknologi digital. Antusiasme peserta terlihat dari tingginya partisipasi selama sesi diskusi, khususnya ketika membahas contoh kasus *phishing*, kebocoran data, dan praktik perlindungan akun digital. Penyampaian materi secara kontekstual membantu peserta memahami bahwa *Ethical Hacking* merupakan upaya legal untuk mengidentifikasi kelemahan sistem guna meningkatkan keamanan, bukan aktivitas peretasan yang melanggar hukum.

Tabel dan Gambar Dokumentasi Kegiatan

Foto	Deskripsi
	Rabu, 25 Februari 2026 Pukul 08.30 – 09.00 Pembukaan Kegiatan Oleh Pembina Yayasan atau Yang Mewakili Bapak P.h.a.y. Johnson Riberu, S.Si dan Bapak Edwin Lesmana Tjiong, B. Eng, M.Com selaku Ketua Lembaga Penelitian dan Pengabdian Kepada Masyarakat Universitas Kalbis.
	Rabu, 25 Februari 2026 Pukul 09.00 – 11.30 Pelatihan dengan Topik Keamanan Siber dan Pemrograman Gim Kegiatan Oleh Bapak Harya Bima Dirgantara, S.T., M.T.I., Edwin Lesmana Tjiong, B. Eng, M.Com dan Bapak Muhammad Adrinta Abdurrazzaq, S.T., M.T.
	Rabu, 25 Februari 2026 Pukul 11.30 – 12.00 Penutupan Pelatihan oleh Bapak P.h.a.y. Johnson Riberu, S.Si dan Bapak Edwin Lesmana Tjiong, B. Eng, M.Com.

Sumber: Olahan Tim Penulis, 2026

B. Dampak Pelatihan terhadap Literasi Keamanan Siber

Pelatihan memberikan peningkatan pemahaman peserta mengenai pentingnya keamanan informasi dan perilaku digital yang bertanggung jawab. Peserta mulai memahami bahwa perlindungan data tidak hanya

bergantung pada penggunaan kata sandi yang kuat atau perangkat lunak antivirus, tetapi juga memerlukan kemampuan mengenali potensi kerentanan serta menerapkan praktik keamanan yang tepat. Diskusi mengenai pola pikir *ethical hacker* mendorong siswa untuk berpikir lebih kritis dan sistematis dalam mengidentifikasi risiko di lingkungan digital. Hasil kegiatan menunjukkan bahwa pendekatan edukatif berbasis praktik sederhana efektif dalam meningkatkan kesadaran keamanan siber sekaligus menanamkan nilai integritas dan etika sebagai landasan penggunaan teknologi.

IV. KESIMPULAN

Pelatihan *Ethical Hacking* di SMA Kristen Karunia Jakarta berhasil meningkatkan literasi keamanan siber siswa melalui pemahaman mengenai konsep dasar *Ethical Hacking*, identifikasi kerentanan sistem, dan pentingnya etika dalam penggunaan teknologi. Kegiatan ini membentuk pola pikir yang lebih kritis, waspada, dan bertanggung jawab terhadap ancaman digital. Ke depan, pelatihan serupa perlu dilakukan secara berkelanjutan dengan materi yang lebih aplikatif agar kemampuan keamanan siber siswa terus berkembang seiring meningkatnya tantangan di era transformasi digital.

DAFTAR RUJUKAN

- EC-Council. (2021). *Certified Ethical Hacker (CEH) Version 11 Study Guide*. Cengage Learning.
- Kementerian Komunikasi dan Informatika Republik Indonesia (2025). *Indeks Masyarakat Digital Indonesia (IMDI) 2025: Akselerasi talenta digital dan ketahanan siber*. Kementerian Komunikasi dan Informatika R.I.
- Pemerintah Republik Indonesia (2024). *UU Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara R.I.
- Purbo, O. W. (2023). *Keamanan jaringan internet: Panduan ethical hacking untuk pemula*. Andi Offset.
- S'to. (2021). *Cyber security untuk pemula: Mengenal hacker mindset dan pertahanan sistem*. Jasakom.
- Waid, A. (2022). *Etika dunia maya: Membangun integritas digital di lingkungan pendidikan menengah*. Pustaka Media.