



Ethical Hacking Sebagai Strategi Keamanan Cyber di Era Digital: Studi Pustaka dan Implementasi Dasar

Kristofel Santa ^{1*}, Enjelita Radjakore ², Rikna Aresta Lahutung ³,
Ravila Putri Pangalila ⁴, Tresya Veronika Deil ⁵

¹⁻⁵ Program Studi Teknik Informatika, Universitas Negeri Manado, Indonesia

Email: kristofelsanta@unima.ac.id, 21210011@unima.ac.id, 21210015@unima.ac.id, 21210151@unima.ac.id,
21210134@unima.ac.id

Abstract Cyber security is becoming a crucial issue in the digital age, especially with the increasing number of cyber attacks on information systems in the public and private sectors. Ethical hacking or ethical hacking is one of the approaches that is beginning to be widely applied to identify and close security gaps in systems. This article discusses the basic concepts of ethical hacking, the process of its implementation, and its urgency in securing information systems. This study was conducted through a literature study approach from various academic and technical sources. The results show that ethical hacking can significantly reduce the potential for cyberattacks with a systematic preventive approach. The study also highlights the importance of legality and Ethics in its implementation, as well as the need for supportive policies at the institutional level.

Keywords: Ethical Hacking, Cyber Security, Penetration Testing, White Hat, Information Systems

Abstrak Keamanan Cyber menjadi isu krusial di era digital, terutama dengan meningkatnya jumlah serangan siber terhadap sistem informasi di sektor publik maupun swasta. Ethical hacking atau peretasan etis adalah salah satu pendekatan yang mulai banyak diterapkan untuk mengidentifikasi dan menutup celah keamanan dalam sistem. Artikel ini membahas konsep dasar ethical hacking, proses pelaksanaannya, dan urgensinya dalam pengamanan sistem informasi. Studi ini dilakukan melalui pendekatan studi pustaka dari berbagai sumber akademik dan teknis. Hasilnya menunjukkan bahwa ethical hacking mampu secara signifikan mengurangi potensi serangan siber dengan pendekatan preventif yang sistematis. Penelitian ini juga menyoroti pentingnya legalitas dan etika dalam pelaksanaannya, serta perlunya kebijakan yang mendukung di tingkat institusi.

Kata Kunci: Ethical Hacking, Keamanan Cyber, Penetration Testing, White Hat, Sistem Informasi

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat memunculkan berbagai tantangan baru dalam hal keamanan data dan sistem informasi. Salah satu tantangan utamanya adalah meningkatnya intensitas dan kompleksitas serangan cyber. Data dari Badan cyber dan Sandi Negara (BSSN) tahun 2024 menunjukkan lebih dari 300 juta serangan siber terjadi di Indonesia. Dalam konteks ini, ethical hacking menjadi salah satu pendekatan yang efektif untuk mencegah serangan dengan mengidentifikasi celah sistem sebelum dimanfaatkan oleh pihak tidak bertanggung jawab.

Ethical hacking merupakan praktik peretasan yang dilakukan secara legal dan etis oleh seorang profesional (ethical hacker) dengan izin dari pemilik sistem. Tujuan utamanya adalah untuk menguji keamanan sistem dan memberikan solusi perbaikan terhadap kerentanan yang

ditemukan. Artikel ini bertujuan untuk mengeksplorasi konsep ethical hacking dan urgensinya sebagai strategi keamanan siber.

Dalam era digital yang terus berkembang pesat, keamanan informasi menjadi aspek yang sangat krusial bagi kelangsungan operasional berbagai sektor, baik pemerintahan, pendidikan, kesehatan, maupun industri. Ketergantungan yang tinggi terhadap sistem informasi berbasis jaringan menjadikan setiap celah keamanan sebagai potensi ancaman serius. Serangan siber seperti phishing, ransomware, dan DDoS tidak hanya merugikan secara finansial, tetapi juga dapat merusak reputasi institusi dan mengganggu kepercayaan publik.

Data dari Badan Siber dan Sandi Negara (BSSN) tahun 2024 mencatat lebih dari 300 juta insiden siber yang terjadi di Indonesia, mencerminkan tingginya urgensi untuk menerapkan strategi pertahanan yang adaptif dan proaktif. Salah satu pendekatan yang mulai mendapatkan perhatian luas adalah ethical hacking atau peretasan etis.

Ethical hacking merupakan simulasi serangan siber yang dilakukan secara legal dan terkendali oleh pihak profesional (ethical hacker) dengan tujuan mengidentifikasi serta menutup celah keamanan dalam suatu sistem. Berbeda dengan peretas jahat (black hat hacker), ethical hacker bekerja berdasarkan izin resmi dan kode etik yang ketat. Praktik ini memungkinkan organisasi untuk menilai ketahanan sistem mereka sebelum benar-benar diserang pihak eksternal.

Artikel ini bertujuan untuk membahas konsep, tahapan, serta urgensi implementasi ethical hacking sebagai bagian integral dari strategi keamanan siber modern. Selain itu, artikel ini juga menyoroti tantangan legalitas, kesiapan institusi, serta potensi penerapan ethical hacking di lingkungan pendidikan dan organisasi publik sebagai langkah konkret menghadapi dinamika ancaman digital.

2. TINJAUAN PUSTAKA

Ethical hacking berasal dari istilah "white hat hacking", yang berlawanan dengan "black hat hacking" atau peretasan jahat (EC-Council, 2021).

Menurut Kumaret al. (2020), ada lima tahapan utama dalam ethical hacking:

- Reconnaissance pengumpulan informasi awal
- Scanning pemetaan dan identifikasi sistem target
- Gaining Access – eksploitasi celah keamanan
- Maintaining Access – uji kelanjutan serangan

- Covering Tracks – dokumentasi dan penghapusan jejak (untuk simulasi)

Banyak organisasi internasional seperti OWASP dan EC-Council menyediakan standar dan sertifikasi untuk mendukung praktik ethical hacking.

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan studi pustaka (library research), dengan mengumpulkan dan menganalisis referensi dari jurnal ilmiah, buku teks, artikel teknis, dan dokumentasi dari lembaga profesional seperti EC-Council, OWASP, dan ISO/IEC 27001. Analisis dilakukan secara deskriptif-kualitatif untuk merangkum teori, praktik, dan perkembangan terkini dalam ethical hacking.

4. HASIL DAN PEMBAHASAN

Peran Ethical Hacking dalam Keamanan Cyber

Ethical hacking berperan dalam mencegah kebocoran data, melindungi sistem dari serangan malware, dan menjaga integritas sistem informasi. Implementasi penetration testing secara berkala terbukti mengurangi risiko serangan siber hingga 60% pada organisasi yang menerapkannya (CyberEdge, 2023).

Ethical hacking berperan krusial dalam arsitektur keamanan siber kontemporer. Melalui pendekatan berbasis simulasi serangan, praktik ini memberikan sarana bagi organisasi untuk secara proaktif mengidentifikasi serta memperbaiki kerentanan sistem sebelum dimanfaatkan oleh pihak yang berniat jahat.

Legalitas dan Etika

Ethical hacking hanya dapat dilakukan dengan izin tertulis dari pemilik sistem. Tanpa izin, tindakan tersebut tetap dikategorikan sebagai ilegal. Di Indonesia, praktik ethical hacking harus tunduk pada UU ITE, khususnya pasal tentang akses tanpa hak ke sistem elektronik.

Keberhasilan implementasi ethical hacking tidak hanya bergantung pada teknis, namun juga pada aspek legalitas dan etika. Tanpa izin eksplisit dari pemilik sistem, kegiatan tersebut dapat dikategorikan sebagai pelanggaran hukum berdasarkan UU ITE Pasal 30 tentang akses tanpa hak. Oleh karena itu, ethical hacker harus menjunjung tinggi kode etik profesi dan tunduk pada peraturan perundang-undangan yang berlaku.

Organisasi sebaiknya juga menyusun dokumen legal seperti Non-Disclosure Agreement (NDA) dan perjanjian pengujian tertulis sebelum memulai proses ethical hacking.

Implementasi Dasar untuk Institusi

Institusi seperti universitas, rumah sakit, dan instansi pemerintahan dapat mulai menerapkan ethical hacking dengan:

- Melakukan audit sistem informasi secara berkala
- Menggunakan jasa penetration tester bersertifikat
- Menyusun SOP penanganan hasil temuan
- Memberikan pelatihan keamanan siber internal

Institusi pendidikan, layanan kesehatan, dan sektor publik memiliki urgensi tinggi dalam mengadopsi ethical hacking. Implementasi dasar yang dapat dilakukan mencakup:

- Audit keamanan sistem informasi secara berkala
- Kolaborasi dengan tenaga profesional bersertifikasi (CEH, OSCP, dsb.)
- Penyusunan SOP penanganan hasil penetration testing
- Pengembangan program pelatihan keamanan siber internal

Studi kasus menunjukkan bahwa perguruan tinggi yang mengadopsi audit sistem berbasis ethical hacking dapat mengurangi risiko kehilangan data mahasiswa hingga 45% dalam satu tahun penerapan.

Keterbatasan

Beberapa kendala utama dalam implementasi ethical hacking adalah:

- Kurangnya SDM bersertifikat
- Tingginya biaya penetration test profesional
- Kurangnya regulasi nasional khusus terkait ethical hacking

Meski memiliki manfaat signifikan, ethical hacking juga menghadapi sejumlah kendala, antara lain:

- Keterbatasan SDM bersertifikasi: Indonesia masih kekurangan ethical hacker tersertifikasi secara internasional.
- Biaya tinggi: Pengujian penetrasi oleh profesional membutuhkan anggaran besar, yang tidak selalu tersedia di institusi kecil.
- Kurangnya regulasi nasional khusus: Belum adanya undang-undang khusus tentang ethical hacking menghambat adopsi luas di sektor publik.

Meskipun demikian, tantangan ini dapat diatasi melalui kerja sama lintas sektor, peningkatan literasi keamanan, serta dukungan regulasi dari pemerintah

5. KESIMPULAN

Ethical hacking merupakan strategi proaktif yang efektif untuk meningkatkan keamanan sistem informasi. Praktik ini memungkinkan organisasi untuk mengetahui dan memperbaiki kelemahan sistem sebelum disalahgunakan. Meskipun memiliki tantangan dalam aspek legalitas dan biaya, manfaat jangka panjangnya sangat signifikan, terutama dalam konteks peningkatan keamanan data dan sistem digital. Pemerintah dan institusi perlu memberikan dukungan kebijakan, pelatihan, dan sertifikasi agar ethical hacking dapat diterapkan secara luas dan aman.

Ethical hacking merupakan pendekatan strategis dan preventif dalam menjaga keamanan sistem informasi di tengah meningkatnya ancaman siber. Dengan memanfaatkan simulasi serangan yang dilakukan secara legal dan terkendali, organisasi dapat secara proaktif mengidentifikasi serta memperbaiki celah keamanan sebelum disalahgunakan oleh pihak yang tidak bertanggung jawab.

Praktik ethical hacking terbukti efektif dalam menurunkan risiko serangan siber dan mendukung peningkatan ketahanan digital suatu institusi. Namun demikian, penerapannya memerlukan dukungan dari sisi legalitas, ketersediaan sumber daya manusia yang kompeten, serta kebijakan internal yang jelas.

Untuk mendorong implementasi yang lebih luas, diperlukan kolaborasi antara pemerintah, institusi pendidikan, dan sektor industri guna memperkuat regulasi, menyediakan pelatihan serta sertifikasi, dan membangun budaya keamanan siber yang berkelanjutan. Dengan demikian, ethical hacking bukan hanya menjadi solusi teknis, tetapi juga bagian penting dari transformasi digital yang aman dan bertanggung jawab.

DAFTAR PUSTAKA

- Andress, J. (2021). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (3rd ed.). Syngress.
- BSSN. (2024). *Laporan statistik ancaman siber di Indonesia tahun 2024*. Badan Siber dan Sandi Negara Republik Indonesia.
- Chapple, M., & Seidl, D. (2021). *CISSP (ISC)² Certified Information Systems Security Professional official study guide* (9th ed.). Wiley.
- CyberEdge Group. (2023). *Cyberthreat defense report*.
- EC-Council. (2021). *Certified ethical hacker v11 study guide*. EC-Council Press.
- ISO/IEC. (2022). *ISO/IEC 27001:2022 – Information security management systems*.

- Kaur, H., & Singh, J. (2020). Role of ethical hacking in enhancing cybersecurity. *International Journal of Recent Technology and Engineering (IJRTE)*, 8(6), 1558–1562.
- Kumar, R., Sharma, S., & Jain, M. (2020). A comprehensive study on ethical hacking and cyber security. *International Journal of Computer Applications*, 176(18), 1–6.
- Mandiant. (2023). *M-Trends 2023: Cybersecurity trends*.
<https://www.mandiant.com/resources/m-trends>
- NIST. (2020). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology.
- OWASP Foundation. (2022). *OWASP testing guide v4.2*.
- Patel, A., & Prajapati, D. (2020). Vulnerability assessment and penetration testing – An ethical way to strengthen security. *International Journal of Scientific & Technology Research*, 9(4), 1607–1611.
- Sari, L. P., & Nugroho, A. (2022). Analisis implementasi penetration testing pada keamanan sistem informasi perguruan tinggi. *Jurnal Ilmiah Teknologi Informasi*, 18(2), 55–63.
- Sembiring, D., & Siregar, T. (2023). Model pelatihan ethical hacking untuk mahasiswa teknik informatika. *Jurnal Pendidikan Teknologi Informasi*, 6(2), 76–82.
- Wijaya, H., & Putra, R. (2023). Evaluasi keamanan sistem informasi menggunakan metode penetration testing. *Jurnal Teknologi dan Sistem Komputer*, 11(1), 55–63.