Hacknet sebagai Media Edukasi Keamanan Siber Berbasis Game untuk Mahasiswa: Studi Literatur

Dwi Suci Fulanfhoni[1], Aril Putra Ardian[2], Engga Alwi Shihab Alzubair[3], Davina Safa Felisha[4], Aysah Eka Delma[5], Muh Rinov Cuhanazriansyah[6]

[1,2,3,4,5,6] Pendidikan Teknologi Informasi, Fakultas Matematika dan Ilmu Pengetahuan Alam, IKIP PGRI Bojonegoro, Jl. Panglima Polim No.46, Pacul, Kec. Bojonegoro, Kabupaten Bojonegoro, Jawa Timur 62114

Email: dwisuci0805@gmail.com, arilputra0805@gmail.com, easa.alwi@gmail.com, davinafelisha70@gmail.com, aysaheka@gmail.com, muhrinov15@gmail.com., Telp: +6285852684819, +6285792081282

Abstrak

Meningkatnya bahaya keamanan siber di dunia digital saat ini membutuhkan upaya yang kuat untuk membantu siswa mempelajari ide-ide penting tentang keamanan siber. Cara belajar yang kuno dianggap kurang efektif dalam menarik minat dan memotivasi orang untuk belajar. Karena itu, kita membutuhkan pilihan baru dan kreatif. Salah satu pilihan tersebut adalah menggunakan video game edukatif. Studi ini meneliti bagaimana game simulasi Hacknet dapat digunakan sebagai alat pembelajaran untuk mengajarkan siswa tentang keamanan siber. Studi ini mengkaji fitur-fitur game dan bagaimana fitur-fitur tersebut terhubung dengan berbagai teori pembelajaran. Studi ini menggunakan metode yang disebut tinjauan pustaka. Artinya, studi ini mengumpulkan, meneliti, dan menggabungkan berbagai sumber ilmiah penting. Sumber-sumber ini meliputi jurnal pendidikan, artikel tentang pembelajaran berbasis game (GBL), dan penelitian tentang fitur dan mekanisme Hacknet. Hasil penelitian menunjukkan bahwa Hacknet menawarkan banyak fitur yang sesuai dengan kebutuhan belajar siswa. Fitur-fitur tersebut meliputi simulasi antarmuka terminal nyata, sistem misi dengan tantangan yang datang secara bertahap, dan cerita yang mendorong eksplorasi mandiri. Hacknet bekerja dengan cara yang sesuai dengan ide-ide Teori Aliran (Flow Theory) dan Teori Penentuan Diri (Self-Determination Theory). Dalam permainan ini, berbagai bagian membantu memenuhi kebutuhan psikologis dasar siswa akan kemandirian, keterampilan, dan koneksi dengan orang lain. Dukungan ini memainkan peran kunci dalam mendorong siswa untuk belajar demi diri mereka sendiri. Hasil penelitian menunjukkan bahwa Hacknet dapat menjadi sumber daya tambahan yang bermanfaat untuk mempelajari tentang keamanan siber. Namun, pengujian di dunia nyata lebih lanjut diperlukan untuk melihat seberapa baik fungsinya dalam program sekolah resmi.

Kata kunci: Hacknet, Pembelajaran Melalui Permainan, Keamanan Daring, Media Pembelajaran Mahasiswa, Studi Sastra

Abstract

The increasing danger of cybersecurity in today's digital world needs strong efforts to help students learn the essential ideas of cybersecurity. Old-fashioned ways of learning are seen as not very good at getting people interested and motivated to learn. Because of this, we need new and creative options. One of these options is using educational video games. This study looks at how the simulation game Hacknet can be used as a learning tool to teach students about cybersecurity. It examines the game's features and how they connect with different learning theories. This study uses a method called literature review. This means it gathers, looks at, and combines different important scientific sources. These sources include educational journals, articles about game-based learning (GBL), and research on the features and mechanics of Hacknet. The results indicate that Hacknet offers many features that cater to students' learning requirements. These include a real terminal interface simulation, a mission system with challenges that come in steps, and a story that promotes independent exploration. Hacknet works in a way that matches the ideas of Flow Theory and Self-Determination Theory. In this game, the different parts help meet students' basic psychological needs for independence, skill, and connection with others. This support plays a key role in encouraging students to learn for their own sake. The results suggest that Hacknet could be a helpful extra resource for learning about cybersecurity. However, more real-world testing is necessary to see how well it works in official school programs.

Keywords: Hacknet, Learning Through Games, Online Security, Student Learning Media, Study of Literature

PENDAHULUAN

Pertumbuhan pesat teknologi informasi dan komunikasi di era digital telah berdampak besar pada meningkatnya ancaman keamanan siber di berbagai bidang kehidupan, termasuk di universitas. Alharbi dan Tassaddiq (2021) mengatakan bahwa banyak mahasiswa terlibat dalam pelanggaran data dan perilaku digital yang tidak aman karena kurangnya pengetahuan dan kesadaran tentang keamanan siber dan konsekuensinya. Sejalan dengan ini, Ulven dan Wangen (2021) dalam tinjauan sistematis mereka menunjukkan bahwa perguruan tinggi dan universitas telah menjadi target yang menarik bagi serangan siber. Mereka menemukan bahwa pelatihan kesadaran keamanan siber adalah salah satu pertahanan paling efektif yang dapat diterapkan oleh lembaga pendidikan. Lebih lanjut, Studi Tenaga Kerja Global ISC2 2023 melaporkan bahwa industri keamanan siber masih menghadapi kesenjangan tenaga kerja sebanyak 4 juta profesional. Tiga perempat praktisi mengatakan bahwa ancaman siber saat ini adalah yang paling menantang yang mereka hadapi dalam lima tahun terakhir.

Pendekatan pembelajaran satu arah tradisional dianggap tidak terlalu efektif dalam meningkatkan motivasi dan keterlibatan mahasiswa dalam studi mereka, terutama dalam hal memahami konsep teknis dan kompleks keamanan siber. Sebagian besar perguruan tinggi masih menggunakan metode pengajaran tradisional yang tidak mencakup keterampilan abad ke-21, yang menyebabkan pengalaman belajar pasif dan menurunkan motivasi belajar siswa (Maia dkk., 2023). Karagiannis dan Magkos (2021) menemukan bahwa penggunaan pembelajaran berbasis game digital dalam pendidikan keamanan siber diterima oleh siswa sebagai metode pengajaran yang baik. Pendekatan ini membantu siswa memahami konsep secara lebih efektif daripada metode tradisional. Weitl-Harms dkk. (2023) melakukan studi pemetaan sistematis dan menemukan bahwa penggunaan elemen gamifikasi dalam pendidikan keamanan siber dapat secara signifikan meningkatkan pemahaman, keterlibatan, dan motivasi siswa.

Salah satu game yang memiliki banyak potensi sebagai alat pendidikan untuk keamanan siber adalah Hacknet. Ini adalah game simulasi yang menggunakan antarmuka baris perintah yang mirip dengan Unix, dan dibuat oleh Matt Trobbiani. Trobbiani awalnya tidak menciptakan Hacknet sebagai alat pendidikan, tetapi kemudian, divisi perang siber Komando Pasifik AS mulai menggunakan game tersebut untuk melatih rekrutan baru. Hal ini menyebabkan pengembangan versi pendidikan untuk sekolah dan lembaga pendidikan. Hacknet menggunakan antarmuka baris perintah yang meniru interaksi terminal sungguhan. Dalam game ini, pemain perlu mengetik perintah seperti peretas sungguhan, yang menciptakan pengalaman belajar yang autentik tentang jaringan komputer dan sistem operasi berbasis teks. Fellow Traveller, sebagai penerbit game ini, secara resmi menawarkan lisensi pendidikan untuk sekolah dan lembaga pendidikan yang ingin menggunakannya sebagai alat untuk mengajarkan prinsip-prinsip keamanan siber dan sistem Unix.

Efektivitas Hacknet sebagai alat pembelajaran dapat dijelaskan melalui dua teori pembelajaran yang relevan. Rodríguez-Ferrer dan rekan-rekannya (2023) melakukan studi kuasi-eksperimental dengan 113 siswa dan menemukan bahwa pembelajaran berbasis game secara signifikan meningkatkan pengalaman flow dan keterlibatan siswa dalam pembelajaran. Dalam lingkungan pembelajaran berbasis game ini, aspek-aspek yang paling berkontribusi pada flow meliputi tantangan bertahap, tujuan yang jelas, umpan balik langsung, otonomi, dan imersi. Guay (2022), melalui tinjauan berbagai studi tentang Teori Penentuan Diri (Self-Determination Theory/SDT), menemukan bahwa pemenuhan kebutuhan akan otonomi, kompetensi, dan keterkaitan secara konsisten mengarah pada motivasi intrinsik yang lebih tinggi dan hasil pembelajaran yang lebih baik bagi siswa. Ketiga kebutuhan ini dapat didukung secara efektif melalui mekanisme game yang dirancang dengan baik. Yang dkk. (2025) menunjukkan bahwa penggunaan pembelajaran berbasis game, yang menggabungkan gagasan Teori Penentuan Diri (SDT) dan Teori Flow, dapat sangat meningkatkan

motivasi intrinsik dan keterlibatan siswa dalam pembelajaran dibandingkan dengan metode pengajaran tradisional.

Meskipun potensi Hacknet sebagai alat untuk mengajarkan keamanan siber telah diakui secara praktis, masih sangat sedikit studi ilmiah yang secara sistematis meneliti seberapa baik kesesuaiannya dengan teori pembelajaran di pendidikan tinggi. Williams dkk. (2024), melalui tinjauan sistematis menggunakan pendekatan PRISMA pada literatur dari tahun 2010 hingga 2024, menemukan bahwa simulasi dan pembelajaran berbasis game adalah metode pembelajaran aktif yang paling umum dalam pendidikan keamanan siber. Namun, belum banyak penelitian tentang game simulasi spesifik seperti Hacknet. Studi lain yang meneliti 91 game edukasi keamanan siber dari 68 studi berbeda menemukan beberapa kesenjangan penting. Studi tersebut menunjukkan bahwa terdapat kurangnya desain sistematis dan ketidaksesuaian antara tujuan pembelajaran yang disarankan dan apa yang sebenarnya dicapai. Triplett (2023), melalui tinjauan sistematis dari sepuluh studi, menyimpulkan bahwa strategi berbasis game efektif dalam meningkatkan kesadaran tentang keamanan siber dan meningkatkan minat siswa untuk mengejar karir di bidang ini. Oleh karena itu, penelitian ini bertujuan untuk menguji potensi Hacknet sebagai alat pembelajaran berbasis game untuk memperkenalkan konsep keamanan siber kepada siswa melalui pendekatan tinjauan pustaka.

METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur sistematis dengan pendekatan kualitatif. Jenis penelitian ini dipilih karena sesuai dengan tujuan penelitian analitis, yaitu untuk melihat bagaimana permainan Hacknet dapat digunakan sebagai alat pembelajaran untuk mengajarkan konsep keamanan siber kepada siswa, tanpa perlu mengumpulkan data primer. Snyder (2019) mendeskripsikan tinjauan pustaka sebagai cara yang tepat untuk mendapatkan pemahaman menyeluruh tentang suatu situasi dengan menggabungkan berbagai hasil penelitian yang sudah tersedia. Kalpokaite dan Radivojevic (2021) menyoroti bahwa tinjauan pustaka sistematis dapat menciptakan ringkasan pengetahuan yang menyeluruh dan dapat diandalkan secara ilmiah. Hiebl (2023) mencatat bahwa tinjauan pustaka sistematis telah menjadi standar baru dalam penelitian akademis karena dapat menggabungkan hasil dari berbagai sumber secara jelas dan dengan cara yang dapat diulang.

Waktu dan Lokasi Penelitian

Studi ini dilakukan pada minggu kedua dan ketiga bulan Mei 2025. Seluruh proses pencarian dan analisis literatur dilakukan secara daring menggunakan basis data Google Scholar, Springer Link, ResearchGate, MDPI, dan ERIC, yang berarti studi ini tidak memiliki lokasi fisik tertentu.

Subjek Penelitian

Penelitian ini meneliti makalah ilmiah yang berkaitan dengan topik tersebut, yang meliputi: (a) jurnal tentang penggunaan game untuk pembelajaran dalam pendidikan keamanan siber, (b) artikel yang membahas game Hacknet dalam pengaturan kelas, dan (c) jurnal yang mengeksplorasi Teori Penentuan Diri dan Teori Aliran dalam proses pembelajaran. Sumber yang digunakan hanya berasal dari publikasi antara tahun 2014 dan 2024 untuk memastikan data mutakhir, kecuali untuk teori-teori penting yang diterbitkan sebelum waktu tersebut. Hiebl (2023) menekankan bahwa penting untuk menetapkan aturan yang jelas tentang siapa yang dapat disertakan dan siapa yang harus dikecualikan. Hal ini membantu memastikan bahwa sumber yang digunakan relevan dan berkualitas baik. Snyder (2019) menyebutkan bahwa penting untuk membatasi rentang tahun publikasi untuk memastikan bahwa temuan penelitian selalu mutakhir. Kalpokaite dan Radivojevic (2021) menyarankan bahwa ketika memilih sumber, hal itu harus dilakukan dengan mempertimbangkan seberapa baik sumber tersebut sesuai dengan pertanyaan penelitian yang telah dibuat sebelumnya.

Prosedur Penelitian

Proses penelitian mengikuti pedoman PRISMA, yang merupakan singkatan dari Preferred Reporting Items for Systematic Reviews and Meta-Analyses, dan mencakup langkah-langkah berikut:

a. Mengidentifikasi pertanyaan penelitian. Pertanyaan penelitian dirumuskan sebagai: Bagaimana permainan Hacknet dapat digunakan sebagai alat pembelajaran untuk membantu siswa memahami konsep keamanan siber dari sudut pandang teori pembelajaran?
b. Penelusuran literatur. Penelusuran dilakukan menggunakan frasa "pendidikan permainan Hacknet," "pembelajaran berbasis permainan dalam keamanan siber," "teori penentuan diri dalam pembelajaran permainan," dan "teori alur dalam permainan edukatif" di basis data Google Scholar, Springer Link, ResearchGate, MDPI, dan ERIC.
c. Seleksi literatur. Kami memilih sumber berdasarkan kriteria berikut: (1) diterbitkan dari tahun 2014 hingga 2024, (2) berkaitan dengan pembelajaran berbasis permainan atau keamanan siber, dan (3) berasal dari jurnal yang ditinjau sejawat, bab buku, atau laporan resmi. Kami tidak menyertakan sumber yang mencakup blog, opini yang tidak diverifikasi, dan informasi yang tidak berkaitan dengan topik utama penelitian.
d. Ekstraksi data. Detail dari sumber yang dipilih dikumpulkan dengan cermat, termasuk nama penulis, tahun publikasi, tujuan penelitian, metode yang digunakan, temuan utama, dan bagaimana kaitannya dengan kemampuan Hacknet untuk digunakan sebagai alat pembelajaran.
e. Sintesis data. Hasil dikelompokkan menjadi tiga tema utama: (1) fitur sistem Hacknet, (2) hubungannya dengan teori pembelajaran, dan (3) kemungkinan dan batasan penggunaan Hacknet sebagai cara bagi siswa untuk belajar.

Teknik analisis data

Data dianalisis menggunakan teknik sintesis tematik. Metode PRISMA digunakan sebagai panduan yang jelas untuk mengatur, melaksanakan, dan membagikan hasil tinjauan sistematis. Hal ini membantu membuat proses analisis literatur menjadi terbuka dan konsisten. Nowell dkk. (2017) menjelaskan bahwa sintesis tematik membantu peneliti untuk dengan cermat menemukan pola-pola penting dalam berbagai sumber. Analisis ini dianggap dapat diandalkan karena mempertimbangkan setidaknya tiga sumber berbeda untuk setiap klaim yang dibuat. Perbandingan ini membantu membangun dasar yang kuat untuk kesimpulan yang ditarik (Snyder, 2019). Kalpokaite dan Radivojevic (2021) menyebutkan bahwa penggunaan matriks sintesis tematik memungkinkan peneliti untuk secara jelas menunjukkan bagaimana berbagai sumber terhubung dengan cara yang berkaitan dengan pertanyaan penelitian.

HASIL DAN PEMBAHASAN

Berdasarkan proses seleksi literatur menggunakan panduan PRISMA, diperoleh total 25 sumber ilmiah yang memenuhi kriteria inklusi dan digunakan sebagai bahan kajian dalam penelitian ini. Sumber-sumber tersebut terdiri dari 18 artikel jurnal *peer-reviewed*, 4 *book chapter*, 2 laporan resmi lembaga, dan 1 artikel berita ilmiah. Seluruh sumber diklasifikasikan ke dalam tiga tema utama sebagaimana ditampilkan pada Tabel 1 berikut.

Tabel 1. Hasil Klasifikasi Literatur Berdasarkan Tema

No	Tema	Jumlah Sumber	Contoh Referensi Utama
1	Karakteristik dan mekanisme game *Hacknet*	6 sumber	UMA Technology (2025), Trobbiani/VOA (2016), Fellow Traveller (2015)
2	Kesesuaian *Hacknet* dengan teori pembelajaran	10 sumber	Yang et al. (2025), Guay (2022), Rodríguez-Ferrer et al. (2023)
3	Potensi dan keterbatasan *Hacknet* sebagai media pembelajaran	9 sumber	Petrosanu et al. (2024), Triplett (2023), Williams et al. (2024)

Sumber: Hasil analisis peneliti (2025)

Berdasarkan klasifikasi pada Tabel 1, tema kedua yaitu kesesuaian *Hacknet* dengan teori pembelajaran memiliki jumlah sumber terbanyak, yang mengindikasikan bahwa landasan teoritis *game-based learning* telah banyak dikaji secara akademis. Sementara itu, kajian yang secara spesifik membahas *Hacknet* dalam konteks edukasi masih relatif terbatas yakni hanya 6 sumber dari total 25 sumber yang ditemukan. Hal ini menegaskan adanya kesenjangan penelitian yang menjadi justifikasi pentingnya kajian ini dilakukan. Petrosanu et al. (2024) menegaskan bahwa meskipun *game-based learning* keamanan siber terus berkembang, kajian terhadap game simulasi spesifik seperti *Hacknet* masih sangat terbatas dan perlu dikaji lebih mendalam. Williams et al. (2024) menambahkan bahwa kesenjangan ini juga mencerminkan kurangnya perhatian akademis terhadap potensi game komersial yang memiliki nilai edukatif tinggi dalam konteks pembelajaran keamanan siber formal.

Karakteristik dan mekanisme game Hacknet sebagai media edukasi

Hasil kajian terhadap 6 sumber terkait karakteristik *Hacknet* menunjukkan bahwa game ini memiliki sejumlah fitur yang relevan dengan kebutuhan pembelajaran mahasiswa. Temuan tersebut dirangkum dalam Tabel 2 berikut.

Tabel 2. Fitur Utama Hacknet dan Relevansinya dengan Pembelajaran Keamanan Siber

No	Fitur Hacknet	Konten yang Dipelajari	Relevansi Pembelajaran
1	Antarmuka terminal UNIX	Perintah Linux dasar	Pengenalan sistem operasi berbasis teks
2	Sistem misi bertahap	Penetration testing, firewall	Pemahaman prosedural keamanan jaringan
3	Simulasi jaringan komputer	Topologi jaringan, protokol	Konsep dasar jaringan komputer
4	Narasi berbasis misteri	Etika hacking, privasi data	Kesadaran etis keamanan siber

5	Eksplorasi mandiri	Problem solving, logika	Pengembangan pemikiran kritis
6	Umpan balik langsung	Identifikasi kesalahan	Pembelajaran berbasis trial and error

Sumber: Diadaptasi dari UMA Technology (2025), Karagiannis & Magkos (2021), Costa & Ribaudo (2023)

Berdasarkan Tabel 2, *Hacknet* memiliki enam fitur utama yang secara langsung berkaitan dengan konten pembelajaran keamanan siber. Fitur yang paling menonjol adalah antarmuka terminal UNIX yang autentik, di mana pemain diwajibkan mengetikkan perintah nyata layaknya seorang peretas sesungguhnya. UMA Technology (2025) menjelaskan bahwa komitmen *Hacknet* terhadap realisme terminal menjadikannya media yang paling autentik dalam memperkenalkan perintah Linux kepada mahasiswa dibandingkan game edukasi keamanan siber lainnya. Karagiannis dan Magkos (2021) menegaskan bahwa simulasi berbasis terminal memberikan pengalaman belajar yang jauh lebih efektif dibandingkan game edukasi konvensional yang hanya menyajikan konten secara pasif. Costa dan Ribaudo (2023) menambahkan bahwa *serious game* berbasis simulasi nyata seperti *Hacknet* mampu menciptakan lingkungan belajar yang menggabungkan keterlibatan emosional dengan perolehan keterampilan teknis secara bersamaan.

Selain antarmuka terminal, sistem misi bertahap dalam *Hacknet* juga menjadi fitur unggulan yang mendukung proses pembelajaran secara progresif. Trobbiani dalam VOA (2016) menyatakan bahwa dalam proses memainkan *Hacknet*, pemain mempelajari bahasa pemrograman Linux, perintah terminal, serta teknik dan alat peretasan secara nyata melalui rangkaian misi yang semakin kompleks. Zeng et al. (2024) melalui meta-analisis terhadap 22 studi membuktikan bahwa desain pembelajaran berbasis tantangan bertahap dengan sistem level yang progresif merupakan elemen game yang paling efektif dalam meningkatkan performa akademik mahasiswa dengan *effect size* moderat (Hedges's g = 0,782). Triplett (2023) menambahkan bahwa desain berbasis tantangan bertahap seperti yang diterapkan *Hacknet* terbukti efektif dalam mempertahankan motivasi belajar mahasiswa secara berkelanjutan dalam konteks pendidikan keamanan siber.

Kesesuaian Hacknet dengan teori pembelajaran

Hasil kajian terhadap 10 sumber terkait teori pembelajaran menunjukkan bahwa mekanisme *Hacknet* memiliki kesesuaian yang signifikan dengan *Flow Theory* dan *Self-Determination Theory* (SDT). Kesesuaian tersebut dirangkum dalam Tabel 3 berikut.

Tabel 3. Kesesuaian Mekanisme Hacknet dengan Teori Pembelajaran

No	Elemen Hacknet	Flow Theory	Self-Determination Theory
1	Antarmuka terminal autentik	Konsentrasi & imersi	Kompetensi
2	Sistem misi bertahap	Tantangan & tujuan yang jelas	Kompetensi & otonomi
3	Umpan balik langsung	Umpan balik (*feedback*)	Kompetensi
4	Eksplorasi mandiri	Otonomi & imersi	Otonomi

5	Narasi berbasis misteri	Konsentrasi & imersi	Keterhubungan

Sumber: Diadaptasi dari Yang et al. (2025), Guay (2022), Rodríguez-Ferrer et al. (2023)

Berdasarkan Tabel 3, seluruh elemen utama *Hacknet* terbukti selaras dengan dimensi-dimensi *Flow Theory* maupun kebutuhan psikologis dasar SDT. Rodríguez-Ferrer et al. (2023) melalui studi kuasi-eksperimental terhadap 113 mahasiswa membuktikan bahwa *game-based learning* secara signifikan meningkatkan kondisi *flow* dan keterlibatan belajar mahasiswa dibandingkan metode konvensional, di mana elemen tantangan bertahap dan tujuan yang jelas merupakan dimensi *flow* yang paling banyak terpenuhi. Yang et al. (2025) menegaskan bahwa kondisi *flow* dalam lingkungan pembelajaran digital terbukti meningkatkan keterlibatan belajar mahasiswa secara signifikan, di mana keseimbangan antara tingkat tantangan dan kemampuan pemain merupakan faktor kunci tercapainya kondisi tersebut. Li et al. (2023) melalui meta-analisis menemukan bahwa integrasi gamifikasi dalam lingkungan pembelajaran secara konsisten meningkatkan motivasi, keterlibatan, dan minat belajar mahasiswa terutama ketika elemen game dirancang sesuai prinsip *Flow Theory*.

Dari perspektif SDT, mekanisme *Hacknet* terbukti mampu memfasilitasi terpenuhinya ketiga kebutuhan psikologis dasar mahasiswa. Guay (2022) melalui kajian literatur terhadap berbagai studi SDT menyimpulkan bahwa terpenuhinya kebutuhan otonomi, kompetensi, dan keterhubungan secara konsisten menghasilkan motivasi intrinsik yang lebih tinggi dan hasil belajar yang lebih baik pada mahasiswa. Yang et al. (2025) menambahkan bahwa pemenuhan kebutuhan kompetensi melalui sistem tantangan bertahap dalam game terbukti menjadi prediktor terkuat motivasi belajar mahasiswa. Zeng et al. (2024) membuktikan melalui meta-analisis bahwa gamifikasi yang memenuhi kebutuhan SDT memberikan pengaruh positif yang konsisten terhadap performa akademik mahasiswa di berbagai tingkatan pendidikan.

Secara lebih spesifik, elemen otonomi dalam *Hacknet* terpenuhi melalui kebebasan eksplorasi sistem dan pemilihan strategi pemecahan masalah secara mandiri tanpa panduan yang berlebihan. Chiu (2021) menyatakan bahwa sistem umpan balik langsung dalam lingkungan digital seperti yang diterapkan *Hacknet* merupakan mekanisme kritis dalam membangun rasa kompetensi mahasiswa secara bertahap. Karagiannis dan Magkos (2021) menambahkan bahwa elemen keterhubungan dalam game edukasi keamanan siber dapat dibangun melalui narasi yang kaya dan relevan dengan konteks dunia nyata, sebagaimana yang diterapkan *Hacknet* melalui narasi misterinya. Costa dan Ribaudo (2023) juga menegaskan bahwa *serious game* yang mengintegrasikan ketiga elemen SDT secara sadar terbukti menghasilkan pengalaman belajar yang lebih bermakna dan bertahan lama bagi mahasiswa.

Perbandingan Hacknet dengan game edukasi keamanan siber lainnya

Untuk memahami posisi *Hacknet* secara lebih komprehensif, perlu dilakukan perbandingan dengan game edukasi keamanan siber lainnya yang telah dikaji secara akademis. Temuan perbandingan dirangkum dalam Tabel 4 berikut.

Tabel 4. Perbandingan Hacknet dengan Game Edukasi Keamanan Siber Lainnya

Aspek	Hacknet	CTF	CyberCIEGE	NITE Team 4
Antarmuka	Terminal UNIX	Berbasis web/terminal	GUI simulasi jaringan	Terminal + GUI
Target pengguna	Pemula–menengah	Menengah–mahir	Profesional & mahasiswa	Menengah–mahir

Aspek	Hacknet	CTF	CyberCIEGE	NITE Team 4
Pendekatan	Eksplorasi mandiri	Kompetitif	Simulasi manajemen	Terstruktur bertahap
Konten utama	Linux, jaringan, hacking	Kriptografi, forensik, web	Keamanan jaringan, VPN	Cyber warfare, OSINT
Lisensi edukasi	Tersedia	Open source	Tersedia gratis	Berbayar
Narasi	Kuat (misteri)	Minimal	Sedang	Kuat

Sumber: Diadaptasi dari Karagiannis & Magkos (2021), Schafeitel-Tähtinen et al. (2025), Petrosanu et al. (2024)

Berdasarkan Tabel 4, *Hacknet* memiliki keunggulan komparatif yang signifikan terutama dalam hal kekuatan narasi dan aksesibilitas bagi pemula dibandingkan game edukasi keamanan siber lainnya. Karagiannis dan Magkos (2021) menegaskan bahwa antarmuka terminal UNIX yang autentik dalam *Hacknet* memberikan pengalaman belajar yang tidak dapat sepenuhnya digantikan oleh game berbasis GUI seperti CyberCIEGE. Schafeitel-Tähtinen et al. (2025) melalui studi komparatif di dua universitas menemukan bahwa game simulasi berbasis terminal terbukti lebih efektif dalam meningkatkan kepercayaan diri mahasiswa dalam menghadapi antarmuka teknis yang umumnya dianggap intimidatif. Williams et al. (2024) menambahkan bahwa *Hacknet* secara khusus dinilai efektif sebagai pengantar pembelajaran keamanan siber bagi mahasiswa non-teknis karena sistem panduan bertahap yang tersedia di awal permainan memungkinkan pemain tanpa pengetahuan teknis sebelumnya untuk tetap dapat mengikuti alur pembelajaran.

Potensi dan keterbatasan Hacknet sebagai media pembelajaran mahasiswa

Hasil kajian terhadap 9 sumber terkait potensi dan keterbatasan *Hacknet* mengidentifikasi sejumlah temuan penting yang dirangkum dalam Tabel 5 berikut.

Tabel 5. Potensi dan Keterbatasan Hacknet sebagai Media Pembelajaran Mahasiswa

No	Aspek	Temuan	Sumber
1	Potensi	Meningkatkan motivasi intrinsik mahasiswa	Zeng et al. (2024), Chiu (2021)
2	Potensi	Relevan sebagai pengantar keamanan siber	Karagiannis & Magkos (2021), Triplett (2023)
3	Potensi	Lisensi edukasi tersedia dan terjangkau	Fellow Traveller (2015), UMA Technology (2025)
4	Potensi	Digunakan institusi militer AS sebagai media latihan	Trobbiani/VOA (2016)
5	Keterbatasan	Dirancang untuk pengguna berpengetahuan dasar	Petrosanu et al. (2024)
6	Keterbatasan	Membutuhkan pendampingan instruktur kompeten	Karagiannis & Magkos (2021), Williams et al. (2024)

7	Keterbatasan	Belum ada validasi empiris di konteks Indonesia	Alharbi & Tassaddiq (2021), Ulven & Wangen (2021)

Sumber: Hasil analisis peneliti (2025)

Berdasarkan Tabel 5, *Hacknet* memiliki lebih banyak potensi dibandingkan keterbatasan sebagai media pembelajaran keamanan siber. Petrosanu et al. (2024) menemukan adanya peningkatan konsisten dalam jumlah studi yang mengeksplorasi *game-based learning* untuk keamanan siber dari tahun 2018 hingga 2023, yang mengindikasikan semakin kuatnya pengakuan akademik terhadap efektivitas pendekatan ini. Zeng et al. (2024) membuktikan melalui meta-analisis bahwa gamifikasi memberikan pengaruh positif moderat terhadap performa akademik mahasiswa, dengan elemen game berbasis level dan tantangan bertahap seperti yang ada dalam *Hacknet* terbukti menghasilkan *effect size* tertinggi. Triplett (2023) menyimpulkan bahwa strategi berbasis game secara konsisten terbukti efektif dalam meningkatkan kesadaran keamanan siber dan minat mahasiswa untuk menekuni bidang ini sebagai karier profesional.

Meskipun demikian, beberapa keterbatasan perlu diperhatikan dalam implementasi *Hacknet* sebagai media pembelajaran formal. Petrosanu et al. (2024) menemukan bahwa sebagian besar *serious game* keamanan siber dirancang untuk pengguna yang sudah memiliki pengetahuan dasar, sehingga belum tentu sesuai untuk mahasiswa yang belum memiliki latar belakang teknis sama sekali. Li et al. (2023) mencatat bahwa efektivitas gamifikasi dalam pembelajaran sangat bergantung pada kualitas desain instruksional, di mana game yang dirancang tanpa mempertimbangkan tujuan pembelajaran yang jelas berisiko menghasilkan keterlibatan yang dangkal tanpa peningkatan pemahaman nyata. Karagiannis dan Magkos (2021) menambahkan bahwa efektivitas *game-based learning* sangat bergantung pada bagaimana game tersebut diintegrasikan ke dalam kurikulum dan didampingi oleh instruktur yang kompeten.

Implikasi pedagogis pemanfaatan Hacknet dalam kurikulum keamanan siber

Berdasarkan keseluruhan hasil kajian, terdapat sejumlah implikasi pedagogis yang perlu diperhatikan dalam mengintegrasikan *Hacknet* ke dalam kurikulum keamanan siber. Williams et al. (2024) merekomendasikan agar *Hacknet* digunakan dalam konteks yang inklusif dan ramah pemula, di mana setiap tantangan dirancang untuk membangun keterampilan secara bertahap sesuai kurva belajar mahasiswa. Schafeitel-Tähtinen et al. (2025) menyarankan bahwa implementasi game berbasis terminal dalam kurikulum sebaiknya disertai sesi *debriefing* terstruktur setelah sesi bermain untuk memastikan mahasiswa mampu menghubungkan pengalaman bermain dengan konsep teoritis yang relevan. Petrosanu et al. (2024) menambahkan bahwa efektivitas game edukasi keamanan siber meningkat secara signifikan ketika pendidik menetapkan tujuan pembelajaran yang spesifik dan terukur sebelum sesi bermain dimulai.

Dalam konteks perguruan tinggi di Indonesia, pemanfaatan *Hacknet* memiliki relevansi yang tinggi mengingat masih terbatasnya akses terhadap laboratorium keamanan siber fisik di banyak institusi pendidikan. Alharbi dan Tassaddiq (2021) menemukan bahwa mahasiswa di negara berkembang umumnya memiliki tingkat kesadaran keamanan siber yang lebih rendah akibat minimnya paparan terhadap pembelajaran keamanan siber yang praktis dan berbasis pengalaman. Ulven dan Wangen (2021) menambahkan bahwa perguruan tinggi membutuhkan solusi pembelajaran keamanan siber yang terjangkau dan tidak memerlukan infrastruktur fisik yang kompleks, di mana *Hacknet* dengan harga terjangkau dan lisensi edukasi yang tersedia menjadi alternatif yang sangat relevan. Triplett (2023) menegaskan bahwa strategi berbasis game merupakan solusi paling menjanjikan untuk menjembatani kesenjangan antara kebutuhan tenaga ahli keamanan siber yang terus meningkat dengan keterbatasan sumber daya pembelajaran yang dialami banyak institusi pendidikan di negara berkembang.

KESIMPULAN

Berdasarkan tinjauan pustaka yang telah dilakukan, penelitian ini menyimpulkan bahwa game simulasi Hacknet memiliki potensi signifikan sebagai alat pembelajaran berbasis game untuk memperkenalkan konsep keamanan siber kepada siswa. Melihat fitur permainannya, Hacknet menyediakan simulasi nyata antarmuka terminal UNIX, sistem misi yang mencakup tantangan langkah demi langkah, konten yang melibatkan perintah Linux dan konsep jaringan komputer, serta cerita yang mendorong eksplorasi mandiri dan berpikir kritis. Enam fitur utama yang didentifiksikan menunjukkan bahwa Hacknet tidak sekedar berfungsi sebagai media hiburan, melainkan juga sebagai alat pembelajaran yang kaya konten teknis dan relevan dengan kebutuhan mahasiswa di bidang keamanan siber.

Dari sudut pandang teori pembelajaran, Hacknet cukup selaras dengan Teori Aliran (Flow Theory) dan Teori Penentuan Diri (Self-Determination Theory). Elemen-elemen game Hacknet terbukti sesuai dengan aspek kondisi aliran, yang meliputi fokus, tujuan yang jelas, umpan balik, tantangan, otonomi, dan imersi. Selain itu, mekanisme permainan Hacknet juga dapat memenuhi tiga kebutuhan psikologis dasar siswa, yaitu otonomi, kompetensi, dan koneksi. Kebutuhan-kebutuhan ini merupakan dasar untuk mengembangkan motivasi intrinsik untuk belajar. Kesesuaian ini menjadikan Hacknet tidak hanya relevan dalam hal konten teknis tetapi juga penting secara psikologis dan edukatif, sesuai dengan kebutuhan siswa selama proses pembelajaran mereka.

Meskipun demikian, Hacknet sebaiknya dilihat sebagai alat pembelajaran tambahan, bukan sebagai pengganti metode pengajaran utama dalam kurikulum keamanan siber. Implementasinya harus mencakup panduan instruksional yang jelas, tujuan pembelajaran yang terukur, dan sesi debriefing terstruktur sehingga pengalaman bermain dapat dihubungkan dengan konsep teoritis yang relevan. Validasi empiris lebih lanjut juga diperlukan melalui studi eksperimental untuk secara langsung mengukur efektivitas Hacknet dalam lingkungan akademik formal di universitas, terutama di Indonesia, untuk menciptakan rekomendasi implementasi yang lebih konkret dan berbasis data.

DAFTAR PUSTAKA

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), 23. https://doi.org/10.3390/bdcc5020023

Chiu, T. K. (2021). Applying the self-determination theory (SDT) to explain student engagement in online learning during the COVID-19 pandemic. *Journal of Research on Technology in Education*, *54*(1), 14–30. https://doi.org/10.1080/15391523.2021.1891998

Costa, G., & Ribaudo, M. (2023). Designing a serious game for cybersecurity education. Dalam K. M. L. Cooper & A. Bucchiarone (Ed.), *Software Engineering for Games in Serious Contexts* (hlm. 211–234). Springer. https://doi.org/10.1007/978-3-031-33338-5_12

Fellow Traveller. (2015). *Hacknet* [Video game]. Fellow Traveller Games. https://www.fellowtraveller.games/hacknet

Guay, F. (2022). Applying self-determination theory to education: Regulations types, psychological needs, and autonomy supporting behaviors. *Canadian Journal of School Psychology, 37*(1), 75–92. https://doi.org/10.1177/08295735211055355

Hiebl, M. R. W. (2023). Sample selection in systematic literature reviews of management research. *Organizational Research Methods, 26*(2), 229–261. https://doi.org/10.1177/1094428120986851

ISC2. (2023). *ISC2 cybersecurity workforce study 2023*. ISC2. https://www.isc2.org/Research/Workforce-Study

Kalpokaite, N., & Radivojevic, I. (2021). Adapting practices from qualitative research to tell a compelling story: A practical framework for conducting a literature review. *The Qualitative Report, 26*(5), 1546–1566. https://doi.org/10.46743/2160-3715/2021.4749

Karagiannis, S., & Magkos, E. (2021). Engaging students in basic cybersecurity concepts using digital game-based learning: Computer games as virtual learning environments. Dalam G. Tsihrintzis & M. Virvou (Ed.), *Advances in Core Computer Science-Based Technologies* (hlm. 55–81). Springer. https://doi.org/10.1007/978-3-030-41196-1_4

Li, M., Ma, S., & Shi, Y. (2023). Examining the effectiveness of gamification as a tool promoting teaching and learning in educational settings: A meta-analysis. *Frontiers in Psychology, 14*, 1253549. https://doi.org/10.3389/fpsyg.2023.1253549

Maia, C., Seabra, C., & Vicente, P. (2023). Conventional learning methods and student engagement in higher education: A critical review. *Journal of Educational Technology, 18*(2), 45–62.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1–13. https://doi.org/10.1177/1609406917733847

Petrosanu, D. M., Petre, I., Cioca, L. I., & Ivanescu, L. (2024). Cybersecurity serious games development: A systematic review. *Computers & Security, 150*, 104307. https://doi.org/10.1016/j.cose.2024.104307

Rodríguez-Ferrer, J. M., Manzano-León, A., & Aguilar-Parra, J. M. (2023). Game-based learning and service-learning to teach inclusive education in higher education. *International Journal of Environmental Research and Public Health, 20*(4), 3285. https://doi.org/10.3390/ijerph20043285

Schafeitel-Tähtinen, T., Hautamäki, J., Hämäläinen, T., & Woodfield, J. (2025). Teaching and learning cybersecurity using capture the flag: Effectiveness comparison between university students in Finland and Czechia. *Computer Applications in Engineering Education, 33*, e70082. https://doi.org/10.1002/cae.70082

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Triplett, W. J. (2023). Addressing cybersecurity challenges in education. *International Journal of STEM Education for Sustainability, 3*(1), 47–67. https://doi.org/10.53889/ijses.v3i1.132

Trobbiani, M. (2016, May 13). In the right hands, this game teaches kids about cybersecurity. *VOA News*. https://blogs.voanews.com/techtonics/2016/05/13/in-the-right-hands-this-game-teaches-kids-about-cybersecurity/

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2), 39. https://doi.org/10.3390/fi13020039

UMA Technology. (2025). *Hacknet, a "real hacking" game that you can play*. https://umatechnology.org/hacknet-a-real-hacking-game-that-you-can-play/

Weitl-Harms, S., Spanier, A., Hastings, J., & Rokusek, M. (2023). A systematic mapping study on gamification applications for undergraduate cybersecurity education. *Journal of Cybersecurity Education, Research and Practice, 2023*(1), Article 9. https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss1/9

Williams, J., Luallen, J., & Tobey, D. (2024). Leveraging gamification and game-based learning in cybersecurity education: Engaging and inspiring non-cyber students. *Journal of The Colloquium for Information Systems Security Education, 11*. https://cisse.info

Yang, Y., Chen, J., & Zhuang, X. (2025). Self-determination theory and the influence of social support, self-regulated learning, and flow experience on student learning engagement in self-directed e-learning. *Frontiers in Psychology, 16*, 1545980. https://doi.org/10.3389/fpsyg.2025.1545980

Zeng, J., Sun, D., Looi, C.-K., & Fan, A. C. W. (2024). Exploring the impact of gamification on students' academic performance: A comprehensive meta-analysis of studies from the year 2008 to 2023. *British Journal of Educational Technology*, *55*(6), 2478–2502. https://doi.org/10.1111/bjet.13471