Journal of Applied Multimedia and Networking (JAMN)
Vol.x, No.x, Maret 201x, pp. xx~xx
e-ISSN: 2548-6853

ANALISIS TINGKAT EFEKTIVITAS PENGGUNAAN MODUL *WRITE-UP* DALAM MENYELESAIKAN *HACKING LABS*

Adhitya Laksana Prawira[1], Andy Triwinarko, S.T., M.T[2].
*Jurusan Teknik Informatika, Politeknik Negeri Batam
**Program Studi Teknik Rekayasa Multimedia, Politeknik Negeri Batam

Article Info

Article history:

Received Jun 12th, 201x
Revised Aug 20th, 201x
Accepted Aug 26th, 201x

Keyword:

Keamanan siber
Hacking labs
Write-up
Penelitian dan Pengembangan
Modul Pembelajaran

ABSTRAK

Perkembangan teknologi digital pada era Industri 4.0 meningkatkan kebutuhan kompetensi keamanan siber, sementara kesenjangan keterampilan *(cybersecurity skills gap)* antara kebutuhan industri dan kemampuan lulusan perguruan tinggi masih menjadi tantangan. Mahasiswa pemula sering mengalami kesulitan menyelesaikan hacking labs secara mandiri karena pembelajaran masih dominan teoritis dan minim pengalaman praktik langsung. Penelitian ini mengembangkan modul write-up untuk membantu mahasiswa Jurusan Informatika Politeknik Negeri Batam menyelesaikan tantangan *Hacking Labs "Venus"* pada platform *HackMyVM.eu*. Penelitian ini merupakan penelitian dan pengembangan *(Research and Development)* yang mengadaptasi model *4D (Define, Design, Develop, Disseminate)*, dan secara sengaja dibatasi pada tahap Define dan Design, serta proses pembuatan produk pada tahap Develop, tanpa validasi ahli secara formal, uji coba produk kepada mahasiswa, maupun tahap Disseminate, mengingat keterbatasan waktu pelaksanaan penelitian pada masa sidang tugas akhir. Produk yang dihasilkan berupa modul write-up yang mencakup keseluruhan 50 mission pada *Hacking Labs "Venus"*, disusun dengan struktur konsisten dan mencakup enam kategori kompetensi keamanan siber. Kesesuaian produk kemudian dianalisis secara konseptual terhadap tiga prinsip modul pembelajaran efektif, yaitu *self-instructional, adaptive, dan stand-alone.* Hasil analisis menunjukkan bahwa desain modul secara konseptual telah memenuhi ketiga prinsip tersebut. Namun, karena penelitian ini belum melalui tahap validasi ahli maupun uji coba kepada mahasiswa, tingkat efektivitas modul secara empiris belum dapat dipastikan dan direkomendasikan sebagai tindak lanjut penelitian.

Corresponding Author:

Andy Triwinarko, S.T., M.T.
Program Studi Teknik Rekayasa Multimedia, Teknik Informatika.
Politeknik Negeri Batam
Jl. Ahmad Yani, Tlk. Tering, Kec. Batam Kota, Kota Batam, Kepulauan Riau, 29461, Indonesia.
Email: andy@polibatam.ac.id

1. PENDAHULUAN

Perkembangan teknologi digital pada era Industri 4.0 meningkatkan ketergantungan berbagai sektor terhadap sistem komputer dan jaringan internet, sehingga ancaman keamanan siber turut meningkat. Keamanan siber merupakan upaya sistematis untuk melindungi sistem, jaringan, dan data dari ancaman digital yang semakin kompleks, dan kajian sistematis terbaru menegaskan perlunya integrasi antara pendekatan teoretis dan praktik langsung dalam kurikulum pendidikan untuk menutup kesenjangan keterampilan yang timbul akibat percepatan teknologi [1]. Ancaman seperti *malware, phishing, ransomware*, dan *social engineering* menargetkan baik kelemahan teknis maupun faktor manusia dalam suatu organisasi [2], sementara perluasan

permukaan serangan *(attack surface)* akibat transformasi digital menuntut penerapan strategi keamanan yang memadukan deteksi teknis dengan peningkatan kesadaran pengguna [3].

Peningkatan kebutuhan tenaga profesional keamanan siber belum diimbangi oleh kesiapan lulusan perguruan tinggi. Laporan dan studi terkini menegaskan adanya defisit tenaga kerja keamanan siber yang signifikan, sehingga menuntut pendekatan pendidikan dan pelatihan yang lebih pragmatis dan berorientasi pada kompetensi praktis [4]. Selain kompetensi teknis, studi identifikasi keterampilan profesional keamanan siber juga menegaskan bahwa komunikasi, berpikir kritis, dan manajemen proyek merupakan bagian penting dari profil seorang profesional keamanan siber yang kompeten [5].

Salah satu penyebab kesenjangan tersebut adalah metode pembelajaran yang masih dominan teoritis dan minim pengalaman praktik langsung. Aktivitas kompetitif seperti *Capture The Flag (CTF)* telah diidentifikasi sebagai metode pembelajaran praktis yang efektif untuk melatih kemampuan peserta mengidentifikasi celah keamanan, sekaligus menumbuhkan ketekunan dan strategi berpikir sistematis yang dibutuhkan dalam praktik profesional [6]. Cyber range menyediakan lingkungan simulasi interaktif yang menghubungkan teori akademik dengan keterampilan profesional secara lebih realistis dibandingkan metode teoretis murni [7], dan pendekatan yang mengintegrasikan praktik langsung melalui *hands-on labs* maupun cyber range terbukti efektif menghubungkan teori dengan penerapan praktis di bidang keamanan informasi [8].

HackMyVM.eu merupakan salah satu platform hacking labs berbasis virtual machine, dan lab *"Venus"* pada platform tersebut dirancang untuk melatih kemampuan eksploitasi sistem serta pemahaman keamanan jaringan. Meskipun *hacking labs* memberikan pengalaman belajar yang realistis, mahasiswa pemula pada praktiknya sering mengalami kesulitan menyelesaikan tantangan secara mandiri akibat kurangnya pemahaman terhadap alur eksploitasi dan terbatasnya pengalaman penggunaan tools keamanan siber. Media yang dapat digunakan untuk membantu mahasiswa memahami proses penyelesaian hacking labs secara bertahap adalah modul *write-up*, yaitu panduan langkah demi langkah yang menjelaskan tahapan penyelesaian tantangan, penggunaan tools, analisis kerentanan, serta konsep keamanan siber yang terlibat dalam proses eksploitasi. Selain berfungsi sebagai panduan teknis, *write-up* berperan sebagai alat pedagogis yang memperkuat kemampuan berpikir analitis dan pemahaman prosedural peserta, sekaligus menjadi media berbagi pengetahuan antar peserta dalam komunitas keamanan siber [9]. Modul yang dirancang dengan pendekatan *self-directed learning* dan struktur instruksional yang jelas dapat menjadi media belajar efektif untuk mendukung pembelajaran mandiri serta praktik keterampilan teknis [10], dan *e-modul* yang dilengkapi materi, latihan, serta umpan balik terbukti dapat meningkatkan motivasi belajar dan kemandirian mahasiswa [11].

Penelitian terdahulu telah mengkaji efektivitas pembelajaran berbasis tantangan dan modul pembelajaran secara *kuantitatif*. Penerapan *Challenge-Based Learning* terbukti meningkatkan motivasi belajar mahasiswa sebesar 23% dan pemahaman konsep sebesar 18% dibandingkan metode konvensional [12], sementara pembelajaran melalui kompetisi CTF menunjukkan peningkatan rata-rata skor *pretest-posttest* sebesar 20 poin pada kemampuan memahami eksploitasi kerentanan sistem [13]. Kajian mengenai penggunaan write-up secara khusus menunjukkan bahwa mahasiswa yang menyusun dan mempelajari write-up memiliki pemahaman yang lebih baik terhadap mekanisme kerentanan dan eksploitasi sistem dibandingkan mahasiswa yang hanya berpartisipasi tanpa dokumentasi [14]. Penelitian lain juga menunjukkan tingkat efektivitas yang tinggi pada aspek kemandirian belajar dan hasil belajar melalui modul pembelajaran mandiri [15], maupun peningkatan signifikan pada kemampuan analisis kerentanan sistem setelah penggunaan modul praktikum ethical hacking [16]. Meskipun demikian, belum banyak penelitian yang secara khusus menghasilkan produk modul write-up yang konkret disertai analisis kesesuaiannya terhadap prinsip modul pembelajaran efektif, khususnya untuk *hacking labs* pada platform *HackMyVM.eu.*

Berdasarkan kondisi tersebut, penelitian ini bertujuan mengembangkan modul *write-up Hacking Labs "Venus"* sebagai media pembelajaran keamanan siber bagi mahasiswa Jurusan Informatika Politeknik Negeri Batam. Penelitian ini merupakan penelitian dan pengembangan *(Research and Development)* yang menghasilkan produk tertentu sekaligus mengkaji kelayakannya [17], dengan mengadaptasi model *4D (Define, Design, Develop, Disseminate)* yang dikembangkan oleh Thiagarajan, Semmel, dan Semmel [18], mencakup pula prinsip *design and development research* yang menganalisis kondisi yang memengaruhi keberhasilan pengembangan produk pembelajaran [19]. Karena keterbatasan waktu pelaksanaan penelitian pada masa sidang tugas akhir, ruang lingkup penelitian secara sengaja dibatasi hingga tahap *Define* dan *Design*, serta proses pembuatan produk pada tahap *Develop*, tanpa mencakup validasi ahli secara formal, uji coba produk kepada mahasiswa, maupun tahap *Disseminate*. Produk yang dihasilkan kemudian dianalisis kesesuaian konseptualnya terhadap tiga prinsip modul pembelajaran efektif, yaitu *self-instructional, adaptive, dan stand-alone* [11].

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan penelitian dan pengembangan *(Research and Development/R&D)*, yaitu metode yang digunakan untuk menghasilkan produk tertentu sekaligus mengkaji kelayakannya [17], [19]. Model pengembangan yang diadaptasi adalah model *4D (Define, Design, Develop, Disseminate)* yang dikembangkan oleh Thiagarajan, Semmel, dan Semmel [18], karena tahapannya secara khusus dirancang untuk pengembangan bahan/perangkat pembelajaran, relatif ringkas, dan banyak diadaptasi pada penelitian pengembangan modul di pendidikan tinggi vokasi. Penelitian ini dibatasi pada tahap Define, Design, dan proses pembuatan produk pada tahap Develop, tanpa validasi ahli secara formal, uji coba produk kepada mahasiswa, maupun tahap Disseminate.

Tahap *Define* mencakup: (a) front-end analysis, yaitu identifikasi kesenjangan keterampilan keamanan siber dan kesulitan mahasiswa pemula menyelesaikan hacking labs secara mandiri; (b) learner analysis, yaitu penetapan karakteristik sasaran pengguna produk; (c) task analysis dan concept analysis, yaitu identifikasi struktur 50 mission pada Hacking Labs "Venus" beserta konsep keamanan siber yang terlibat pada tiap mission; dan (d) specifying instructional objectives, yaitu perumusan tujuan modul untuk membantu mahasiswa memahami alur eksploitasi dan menyelesaikan seluruh mission secara mandiri.

Tahap *Design* menghasilkan rancangan awal produk, meliputi penyusunan struktur penyajian modul yang konsisten pada setiap mission pernyataan misi, command/tools yang digunakan, tabel penjelasan command, dan bukti penyelesaian penyusunan alur penyajian secara linear-berjenjang mengikuti tingkat kesulitan, serta pemetaan materi ke dalam enam kategori kompetensi keamanan siber.

Tahap *Develop* pada penelitian ini dilaksanakan hanya sampai pada proses realisasi/penyusunan produk akhir modul write-up untuk keseluruhan 50 mission, mengacu pada rancangan yang telah ditetapkan pada tahap *Design*. Ringkasan pelaksanaan tiap tahap ditunjukkan pada Tabel 1.

Tabel 1. Ringkasan Tahapan Model 4D pada penelitian ini

Tahap	Kegiatan	Status
Define	Analisis masalah, sasaran pengguna, tugas/konsep, dan tujuan pembelajaran	Dilaksanakan
Design	Perancangan struktur dan alur penyajian modul	Dilaksanakan
Develop	(a) Realisasi produk; (b) Validasi ahli; (c) Uji coba pengembangan	(a) Dilaksanakan; (b)-(c) tidak dilaksanakan, direkomendasikan untuk penelitian lanjutan
Disseminate	Penyebarluasan produk	Tidak dilaksanakan, di luar ruang lingkup penelitian ini

Sasaran pengguna produk adalah mahasiswa Jurusan Informatika Politeknik Negeri Batam yang telah atau sedang menempuh mata kuliah Keamanan Siber, Sistem Operasi, atau Jaringan Komputer, serta memiliki kemampuan dasar penggunaan sistem Linux. Karakteristik ini merupakan hasil *learner analysis* pada tahap *Define*, bukan sampel penelitian empiris, karena tahap uji coba produk kepada pengguna tidak dilaksanakan pada penelitian ini.

Data pada tahap *Define* dan *Design* dikumpulkan melalui studi literatur mengenai konsep keamanan siber, modul pembelajaran, dan pendekatan *Challenge-Based Learning/Game-Based Learning*; eksplorasi langsung platform *HackMyVM.eu* dan penyelesaian seluruh 50 mission pada *Hacking Labs "Venus"* oleh peneliti sebagai dasar penyusunan konten modul; serta dokumentasi proses penyelesaian setiap mission (command, penjelasan, dan tangkapan layar) sebagai bahan penyusunan produk.

Analisis data bersifat deskriptif-kualitatif, yaitu mencocokkan setiap karakteristik produk (struktur penyajian, alur mission, kelengkapan komponen) terhadap indikator tiga prinsip modul pembelajaran efektif *self-instructional, adaptive, dan stand-alone* [11], [20]. Karena tahap validasi ahli dan uji coba pengguna tidak dilaksanakan, penelitian ini tidak menggunakan instrumen kuantitatif seperti soal *pretest-posttest*, lembar observasi aktivitas, maupun kuesioner persepsi mahasiswa; instrumen tersebut direkomendasikan untuk penelitian lanjutan guna mengukur efektivitas modul secara empiris.

3. HASIL DAN ANALISIS

3.1. Struktur dan Alur Pembelajaran Modul

Modul *Write-Up Hacking Labs Venus* terdiri atas 50 mission yang disusun secara berurutan, di mana penyelesaian satu mission menghasilkan password untuk mengakses user berikutnya, membentuk alur pembelajaran berjenjang *(progressive learning)* yang mencerminkan karakteristik *Challenge-Based Learning.* Setiap mission memiliki struktur penyajian yang konsisten, terdiri atas: (1) judul mission, (2) deskripsi misi, (3) langkah penyelesaian berupa urutan command, (4) penjelasan command beserta parameter yang digunakan, dan (5) hasil penyelesaian berupa password atau akses ke mission berikutnya.

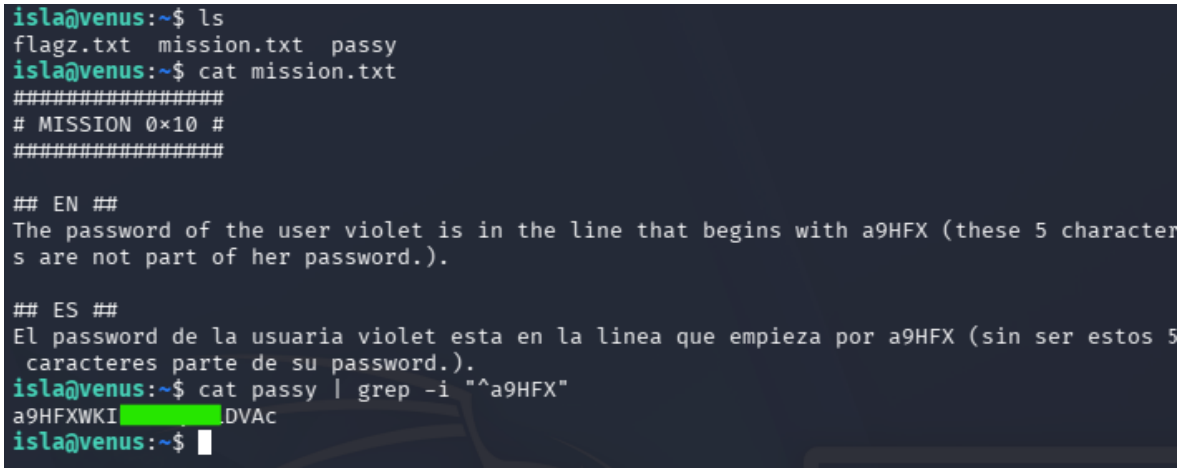
Alur pembelajaran modul mengikuti delapan tahap yang meningkat kompleksitasnya, sebagaimana ditunjukkan pada Gambar 1: *dasar Linux, manipulasi file dan data, privilege dan authentication, web security, database enumeration, digital forensics, password security*, hingga *cryptography* dan *advanced Linux security*. Susunan ini sejalan dengan prinsip learning progression, yaitu materi disampaikan dari konsep sederhana menuju konsep yang lebih kompleks sehingga peserta dapat membangun pengetahuan baru berdasarkan pengalaman belajar sebelumnya [21]. Struktur materi yang disusun secara sistematis dan konsisten pada setiap mission juga meningkatkan *learnability* karena peserta dapat memahami hubungan antar materi dan mengembangkan pengetahuan secara bertahap [20].

3.2. Cakupan Materi dan Penggunaan Command Linux

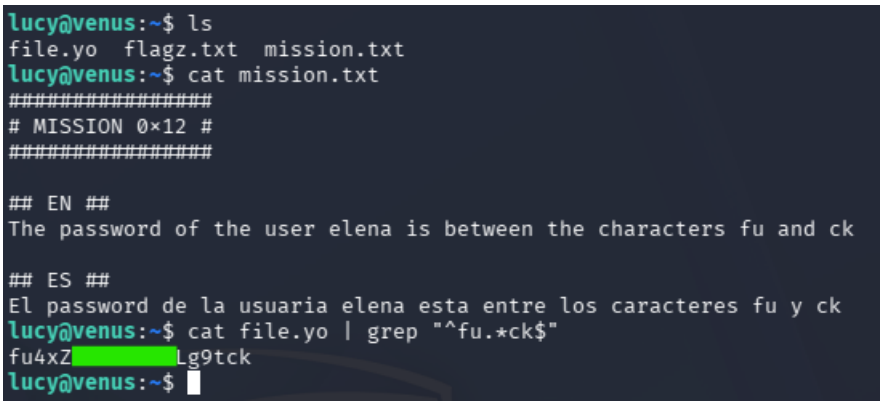
Materi dalam modul dikelompokkan ke dalam sembilan kelompok kompetensi sebagaimana ditunjukkan pada Tabel 2. Setiap mission tidak hanya memuat solusi penyelesaian, tetapi juga penjelasan fungsi command, parameter, maupun konsep keamanan siber yang digunakan sejalan dengan prinsip bahwa materi pembelajaran yang efektif harus menjelaskan konsep yang mendasari suatu aktivitas, bukan hanya prosedur atau langkah kerja [22].

Tabel 2. Klasifikasi Materi Modul *Write-Up Hacking Labs Venus*

Kelompok Materi	Contoh Mission	Kompetensi yang Dipelajari
Dasar Linux	Mission 10–17	Navigasi file, pencarian data, *environment variable*, *file system* Linux
Manajemen File dan Data	Mission 18–24	Kompresi, *encoding*, *decoding*, pencarian file, manipulasi data
Privilege dan Autentikasi	Mission 15, 20, 44, 46	sudo, SSH, *group permission*, doas
Analisis Web	Mission 26, 28, 30, 31, 41, 47	HTTP, *header*, *web service*, DNS
Database	Mission 29	Enumerasi MySQL
Forensik Digital	Mission 21, 22, 27, 34, 37, 45	Metadata, *hexdump*, *binary*, *swap file*, *image*
Password Security	Mission 18, 35, 48	*Password cracking*, *dictionary attack*, *brute force*
Kriptografi	Mission 16, 39, 40	Base64, RSA, Morse Code
Sistem Linux Lanjutan	Mission 25, 32, 42, 43, 49	Bash, *history*, *alias*, DNS *zone*



Gambar 1. Mission 10 (Sumber: Dokumen Pribadi)



Gambar 2. Mission 12 (Sumber: Dokumen Pribadi)

```
denise@venus:~$ ls
flagz.txt  mission.txt
denise@venus:~$ cat mission.txt
################
# MISSION 0×46 #
################

## EN ##
The user zora is screaming doas!

## ES ##
La usuaria zora no deja de gritar doas!
denise@venus:~$ which doas
/usr/bin/doas
denise@venus:~$ doas -u zora whoami
doas (denise@venus) password:
zora
denise@venus:~$ ls
flagz.txt  mission.txt
denise@venus:~$ ls /pwned/zora/
ls: cannot open directory '/pwned/zora/': Permission denied
denise@venus:~$ doas -u zora ls /pwned/zora
doas (denise@venus) password:
flagz.txt  mission.txt  zora_pass.txt
denise@venus:~$ doas -u zora cat /pwned/zora/zora_pass.txt
doas (denise@venus) password:
BWm1R3jCcb53riO
denise@venus:~$
```

Gambar 3. Mission 46 (Sumber: Dokumen Pribadi)

```
zora@venus:~$ ls
flagz.txt  mission.txt  zora_pass.txt
zora@venus:~$ cat mission.txt
################
# MISSION 0×47 #
################

## EN ##
The user belen has left her password in venus.hmv

## ES ##
La usuaria belen ha dejado su password en venus.hmv
zora@venus:~$ cat /etc/hosts
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::  ip6-localnet
ff00::  ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.25.20.20    venus
zora@venus:~$ curl -i -s venus.hmv
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 08 Jul 2026 21:57:14 GMT
Content-Type: text/html
Content-Length: 16
Last-Modified: Mon, 04 May 2026 07:40:45 GMT
Connection: keep-alive
ETag: "69f84d7d-10"
Accept-Ranges: bytes

2j[redacted]wWZ
zora@venus:~$
```

Gambar 4. Mission 47 (Sumber: Dokumen Pribadi)

Hampir seluruh proses penyelesaian mission dilakukan melalui *command line interface*, sehingga command Linux menjadi komponen utama modul. Command yang digunakan meliputi utilitas bawaan *Linux (grep, find, cat, chmod, sudo)* maupun security tools yang umum digunakan dalam praktik *penetration testing (curl, mysql, openssl, hydra, john, exiftool)*. Pembelajaran Linux yang efektif tidak hanya menekankan kemampuan menjalankan command, tetapi juga pemahaman terhadap fungsi, sintaks, dan hubungan antar command sehingga pengguna mampu memilih perintah yang sesuai dengan kebutuhan penyelesaian masalah [23] prinsip yang tercermin dari keberadaan bagian Penjelasan Command pada hampir setiap mission dalam modul.

3.3. Konsep Keamanan Siber

Konsep keamanan siber yang tercakup dalam modul dikelompokkan menjadi sepuluh kategori sebagaimana ditunjukkan pada Tabel 3. Pengelompokan ini sejalan dengan konsep keamanan siber sebagai proses melindungi sistem informasi, jaringan, perangkat, dan data dari akses tidak sah melalui penerapan teknik identifikasi kerentanan, pengelolaan hak akses, perlindungan data, dan pengamanan layanan jaringan [24].

Tabel 3. Konsep Keamanan Siber pada Modul

Konsep	Implementasi pada Modul
Linux System Administration	Navigasi direktori, *file system*, *environment variable*
Information Gathering	Enumerasi file, *database*, DNS, *service*
Authentication	SSH, *password*, *private key*
Authorization	sudo, doas, *group permission*
Web Security	HTTP *request*, HTTP *header*, *localhost*
Database Security	Enumerasi MySQL
Digital Forensics	*Metadata*, *binary file*, *swap file*
Password Security	*Dictionary attack*, *brute force*, *hash cracking*
Cryptography	Base64, RSA, Morse Code
DNS Security	*Local hosts file*, DNS *zone*

Konsep-konsep tersebut tidak berdiri sendiri, melainkan saling berkaitan dalam mendukung penyelesaian mission misalnya, sebelum peserta dapat melakukan *password cracking*, peserta terlebih dahulu harus memahami struktur sistem Linux, pengelolaan berkas, serta autentikasi pengguna. Pembelajaran keamanan siber yang efektif memang harus menghubungkan konsep-konsep dasar sistem operasi, jaringan, kriptografi, autentikasi, dan keamanan aplikasi agar peserta memiliki pemahaman yang utuh terhadap mekanisme pertahanan maupun analisis keamanan suatu sistem [25].

3.4. Kesesuaian Modul dengan Prinsip Modul Pembelajaran Efektif

Analisis kesesuaian dilakukan dengan mencocokkan karakteristik produk terhadap tiga prinsip modul pembelajaran efektif *self-instructional, adaptive, dan stand-alone* [11]. Hasil analisis konseptual ditunjukkan pada Tabel 4.

Tabel 4. Kesesuaian Modul dengan Prinsip Modul Pembelajaran

Tahap	Kegiatan	Status
Define	Analisis masalah, sasaran pengguna, tugas/konsep, dan tujuan pembelajaran	Dilaksanakan
Design	Perancangan struktur dan alur penyajian modul	Dilaksanakan
Develop	(a) Realisasi produk; (b) Validasi ahli; (c) Uji coba pengembangan	(a) Dilaksanakan; (b)-(c) tidak dilaksanakan, direkomendasikan untuk penelitian lanjutan
Disseminate	Penyebarluasan produk	Tidak dilaksanakan, di luar ruang lingkup penelitian ini

Prinsip *self-instructional* terpenuhi karena setiap mission menyajikan langkah penyelesaian yang sistematis, disertai penjelasan fungsi command dan konsep yang mendasarinya, sejalan dengan pandangan bahwa materi pembelajaran mandiri harus memberikan penjelasan yang cukup agar peserta memahami alasan di balik setiap aktivitas, bukan hanya menghafal prosedur [22]. Prinsip *stand-alone* terpenuhi karena modul memuat komponen pembelajaran yang lengkap deskripsi masalah, langkah penyelesaian, penjelasan command, hingga hasil yang diperoleh sehingga dapat digunakan tanpa bergantung pada bahan ajar utama lainnya. Prinsip adaptive terpenuhi karena materi disusun secara bertahap berdasarkan peningkatan kompleksitas dan mencakup berbagai tools yang relevan dengan praktik keamanan siber saat ini [20].

3.5. Pembahasan

Hasil analisis menunjukkan bahwa Modul Write-Up Hacking Labs Venus memiliki struktur yang sistematis, materi yang relevan dengan kompetensi keamanan siber, alur pembelajaran yang bertahap, penggunaan command Linux yang kontekstual, serta integrasi konsep keamanan siber pada setiap mission. Karakteristik ini menjadikan modul lebih sesuai digunakan sebagai media pembelajaran dibandingkan sekadar dokumentasi solusi, karena umumnya write-up yang tersedia pada forum atau blog keamanan siber hanya menyajikan langkah penyelesaian tanpa penjelasan konseptual.

Berbeda dengan penelitian terdahulu yang mengukur efektivitas pembelajaran berbasis tantangan secara kuantitatif melalui pretest-posttest maupun indeks kepuasan pengguna [12], [13], [15], [16], penelitian ini diposisikan sebagai fondasi awal (preliminary study) yang menghasilkan produk modul write-up siap divalidasi. Sejalan dengan temuan bahwa mahasiswa yang mempelajari write-up memiliki pemahaman yang lebih baik terhadap alur eksploitasi [14], produk modul pada penelitian ini dirancang agar setiap langkah penyelesaian disertai penjelasan command dan konsep, bukan sekadar prosedur penyelesaian.

Karena tahap validasi ahli dan uji coba pengguna belum dilaksanakan, kesimpulan kesesuaian pada Tabel 4 bersifat konseptual berdasarkan telaah peneliti (self-review), dan belum dapat digunakan untuk menyimpulkan efektivitas pembelajaran secara empiris. Validasi ahli dan uji coba skala kecil kepada mahasiswa diperlukan pada penelitian lanjutan untuk mengonfirmasi kelayakan dan efektivitas modul ini sebagai media pembelajaran keamanan siber.

4. KESIMPULAN DAN SARAN

Penelitian ini berhasil mengembangkan modul write-up Hacking Labs "Venus" melalui tahap Define, Design, dan proses pembuatan produk pada tahap Develop, mencakup keseluruhan 50 mission pada platform HackMyVM.eu, disusun dalam struktur konsisten berupa pernyataan misi, command, penjelasan command, dan bukti penyelesaian. Materi modul mencakup sembilan kelompok kompetensi keamanan siber, mulai dari navigasi dasar Linux hingga administrasi sistem lanjutan, sehingga memiliki cakupan yang cukup luas untuk mendukung pembelajaran keamanan siber berbasis praktik bagi mahasiswa pemula.

Berdasarkan telaah konseptual peneliti, desain produk modul secara konseptual telah sesuai dengan ketiga prinsip modul pembelajaran efektif, yaitu self-instructional, adaptive, dan stand-alone. Namun, kesesuaian ini belum divalidasi oleh ahli independen maupun diuji langsung kepada mahasiswa sebagai pengguna, sehingga belum dapat disimpulkan sebagai bukti efektivitas modul secara empiris. Penelitian ini menjawab rumusan masalah mengenai rancang bangun modul write-up sesuai ruang lingkup yang telah ditetapkan, yaitu penelitian pengembangan yang dibatasi hingga tahap Define, Design, dan Develop (proses pembuatan produk).

Penelitian lanjutan disarankan untuk melaksanakan validasi ahli (expert judgement) oleh dosen pembimbing atau praktisi keamanan siber, serta uji coba skala kecil kepada mahasiswa melalui pretest-posttest guna mengukur efektivitas modul secara kuantitatif melalui N-Gain, tingkat keberhasilan, efisiensi waktu, dan indeks persepsi mahasiswa. Modul write-up ini juga dapat dipertimbangkan sebagai bahan ajar pendamping pada mata kuliah Keamanan Siber, Sistem Operasi, atau Jaringan Komputer di Politeknik Negeri Batam.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada dosen pembimbing dan kedua dosen penguji, serta Program Studi Teknik Rekayasa Multimedia, Jurusan Teknik Informatika, Politeknik Negeri Batam, atas bimbingan, arahan, dan dukungan yang diberikan selama proses penelitian dan penyusunan artikel ini.

REFERENSI

[1] A. M. Alnajim, *et al.*, "Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches," *Symmetry*, vol. 15, p. 2175, 2023.

[2] M. Abdullah, *et al.*, "Evolution Cybercrime Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data," *Jurnal Analitycs*, vol. 4, pp. 1–25, 2025.

[3] H. P. Maharani, *et al.*, "Peranan Cybersecurity dalam Meningkatkan Ketahanan Bisnis Digital terhadap Cybercrime," *Jurnal Ilmu Ekonomi dan Bisnis*, vol. 3, no. 2, pp. 8–17, 2025.

[4] R. Dillon and K. L. Tan, "Cybersecurity Workforce Landscape, Education and Industry Growth Prospects in Southeast Asia," *Journal of Tropical Futures*, vol. 1, no. 2, pp. 172–181, 2024.

[5] M. Ismail, *et al.*, "Cybersecurity Activities for Education and Curriculum Design: A Survey," *Computers in Human Behavior Reports*, vol. 16, 2024.

[6] A. Tay, *et al.*, "Gamified Cybersecurity Education Through The Lens of The Information Search Process: An Exploratory Study of Capture-The-Flag Competitions," *Informing Science Institute*, vol. 21, 2024.

[7] W. Lazarov, *et al.*, "Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education," 2025.

[8] M. Glas, *et al.*, "Train as you Fight: Evaluating Authentic Cybersecurity Training in Cyber Ranges," in *Proc. CHI '23*, Hamburg, Germany, Apr. 2023.

[9] C. Beauchamp and H. Matusovich, "A Mixed-Method Study Exploring Student Motivation for Participating in Cybersecurity CTF Competitions," *Cybersecurity Pedagogy & Practice Journal*, vol. 3, no. 1, 2024.

[10] V. Yustitia, *et al.*, "Self-Directed Learning Based Teaching Module on Angle Material," *Jurnal Penelitian dan Pengembangan Pendidikan*, vol. 8, no. 3, pp. 612–620, 2024.

[11] T. Sidauruk, *et al.*, "E-Modules to Improve Learning Independence, Motivation and Learning Outcomes," *Jurnal Penelitian dan Pengembangan Pendidikan*, vol. 9, no. 1, pp. 171–180, 2025.

[12] A. Pratama and B. Rachman, "Penerapan Challenge-Based Learning dalam Pembelajaran Keamanan Jaringan," *Jurnal Inovasi Teknologi Pembelajaran*, vol. 8, no. 3, pp. 210–220, 2021.

[13] D. Wijaya, N. Sari, and A. Putra, "Efektivitas Pembelajaran Game-Based Learning pada Kompetisi Capture The Flag (CTF)," *Jurnal Pendidikan Informatika*, vol. 11, no. 1, pp. 55–67, 2022.

[14] D. Nugroho, "Analisis Penggunaan Write-Up Sebagai Media Refleksi Pembelajaran di Kompetisi Capture The Flag," *Jurnal Keamanan Siber dan Informatika*, vol. 4, no. 1, pp. 45–56, 2022.

[15] Y. Ramadhan and A. Yusuf, "Analisis Efektivitas Penggunaan Modul Pembelajaran Mandiri pada Mata Kuliah Jaringan Komputer," *Jurnal Pendidikan Vokasi*, vol. 9, no. 1, pp. 33–42, 2023.

[16] T. Setiawan and I. Prakoso, "Evaluasi Efektivitas Modul Pembelajaran Berbasis Praktikum pada Materi Ethical Hacking," *Jurnal Teknologi dan Sistem Informasi*, vol. 7, no. 2, pp. 98–107, 2021.

[17] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta, 2019.

[18] S. Thiagarajan, D. S. Semmel, and M. I. Semmel, *Instructional Development for Training Teachers of Exceptional Children: A Sourcebook*. Bloomington, IN: Indiana University, 1974.

[19] R. C. Richey and J. D. Klein, *Design and Development Research: Methods, Strategies, and Issues*. New York: Routledge, 2007.

[20] R. M. Branch and T. A. Dousay, *Survey of Instructional Design Models*, 6th ed. Bloomington, IN: AECT, 2022.

[21] M. D. Merrill, *First Principles of Instruction: Identifying and Designing Effective, Efficient, and Engaging Instruction*. Hoboken, NJ: Wiley, 2023.

[22] W. Horton, *E-Learning by Design*, 3rd ed. Hoboken, NJ: Wiley, 2021.

[23] W. E. Shotts, *The Linux Command Line*, 2nd ed. San Francisco, CA: No Starch Press, 2022.

[24] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD: U.S. Dept. of Commerce, 2024.

[25] W. Stallings, *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Boston, MA: Addison-Wesley, 2022.