BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang sangat cepat telah mengubah segala aspek kehidupan manusia. Internet pada awalnya menjadi dasar bagi perubahan dan peluang yang besar dalam konektivitas global. Seseorang dapat terhubung dengan siapa pun, di mana pun, dan membuka peluang untuk pertukaran informasi yang tak terbatas. Selanjutnya perkembangan teknologi juga menciptakan peluang baru di bidang teknologi dan digital seperti pengembang perangkat lunak, analisis data, ahli keamanan *cyber*, dan pemasaran digital (Lubis & Nasiton, 2023).

Seiring dengan perkembangan teknologi dan terciptanya hal baru, selalu terdapat konsekuensi baru yang mengiringinya. Kecanggihan teknologi kemudian memunculkan istilah-istilah baru, salah satunya adalah *cybersecurity*. Pengetahuan mengenai *cybersecurity* sangat penting karena masyarakat dituntut beradaptasi dengan teknologi, mengingat manusia dan teknologi saling berkaitan satu sama lain. *Cybersecurity* memiliki peran yang sangat penting untuk menemukan, memperbaiki ataupun mengurangi risiko terjadinya ancaman *cyber* yang dapat mengancam seluruh data dan komponen sistem *cyber* itu sendiri (Rosihan et al., 2023).

Pendidikan *cybersecurity* sangat penting bagi semua siswa, mulai dari sekolah dasar hingga perguruan tinggi, termasuk bagi orang dewasa yang ingin memahami keamanan digital (Khalid et al., 2018). Salah satu cara untuk meningkatkan keterampilan pada bidang ini adalah dengan menyediakan laboratorium sebagai tempat belajar dan praktik langsung yang aman. Pada lingkungan perguruan tinggi, kebutuhan akan teknologi informasi terus berkembang, terutama untuk mendukung praktikum *cybersecurity*. Namun, akses ke laboratorium fisik hanya dapat dilakukan di tempat dan waktu tertentu, sehingga membatasi fleksibilitas pembelajaran.

Untuk mengatasi keterbatasan tersebut, diperlukan solusi yang memungkinkan pelajar dapat mengakses komputer laboratorium kapan saja dan dari mana saja tanpa harus datang ke laboratorium fisik. Oleh karena itu, penelitian ini bertujuan untuk memanfaatkan komputer yang ada pada program studi sebagai laboratorium virtual berbasis Proxmox VE, sehingga pelajar atau mahasiswa dapat melakukan praktikum *cybersecurity* dengan lebih fleksibel, aman, dan tanpa keterbatasan ruang serta waktu.

Laboratorium virtual adalah sebuah simulasi lingkungan yang dibangun menggunakan teknologi virtualisasi sehingga pengguna dapat belajar metode *cybersecurity*, melakukan pengujian serangan dan memperoleh keterampilan untuk mendeteksi, mencegah dan mengatasi ancaman *cyber* di lingkungan ini. Dengan menggunakan metode virtualisasi, laboratorium *cybersecurity* dapat mengoptimalkan jumlah penggunaan komputer fisik. Salah satu platform yang dapat digunakan untuk membangun lingkungan virtual ini adalah Proxmox *Virtual Environment*.

x VE dalam penelitian ini didasarkan pada beberapa keunggulan erdasarkan penelitian yang dilakukan oleh Nuryadin et al., (2023) kkan kinerja CPU, memori, respons waktu dan penggunaan *disk* gkan teknologi virtualisasi lainnya. Proxmox VE juga dianggap ebih baik dalam menjalankan web server.

an masalah yang telah dijelaskan sebelumnya, maka penulis hir dengan judul "IMPLEMENTASI PROXMOX VE UNTUK

LABORATORIUM VIRTUAL *CYBERSECURITY* PADA PROGRAM STUDI SISTEM INFORMASI FMIPA UNIVERSITAS HASANUDDIN". Tugas akhir ini sebagai bentuk pengembangan sistem yang ada sebelumnya untuk memaksimalkan komputer yang ada pada program studi. Dengan adanya sistem ini, diharapkan proses pembelajaran dan praktik pada laboratorium komputer bisa dilakukan di mana saja, lebih mudah dan efisien.

1.2 Rumusan Masalah

Berdasarkan uraian di atas, dapat dirumuskan beberapa masalah yang dihadapi dalam pembuatan tugas akhir yaitu sebagai berikut:

1. Bagaimana merancang sebuah laboratorium *cybersecurity* virtual pada Prodi Sistem Informasi?
2. Bagaimana mengefisienkan penggunaan sumber daya pada Proxmox agar dapat dioptimalkan untuk mendukung operasional laboratorium virtual dengan keterbatasan perangkat keras?
3. Bagaimana menguji laboratorium *cybersecurity* virtual agar berjalan dengan baik dalam mempraktikkan *cybersecurity*?

1.3 Batasan Masalah

Dalam menganalisis dan merancang laboratorium virtual ini diperlukan pembatasan agar tidak menyimpang dari topik yang diambil. Berikut masalah yang dibatasi adalah:

1. Penelitian ini menggunakan Proxmox VE sebagai lingkungan virtual untuk Laboratorium *cybersecurity* virtual.
2. *Virtual Machine* yang dibuat dalam laboratorium virtual *cybersecurity* menggunakan distribusi Linux.
3. Menggunakan komputer pada laboratorium komputer Sistem Informasi Universitas Hasanuddin.

1.4 Tujuan Penelitian

Adapun tujuan penelitian ini adalah sebagai berikut:

1. Merancang laboratorium *cybersecurity* virtual pada Program Studi Sistem Informasi.
2. Melakukan pengujian untuk mengetahui berapa maksimal VM yang dapat dijalankan pada laboratorium virtual menggunakan komputer Program Studi Sistem Informasi.
3. Menguji laboratorium *cybersecurity* virtual agar dapat berjalan dengan baik.

1.5 Manfaat Penelitian

Berdasarkan permasalahan yang telah dirumuskan, maka manfaat dari tugas akhir ini adalah:

1. Memberikan kontribusi dalam pengembangan pengetahuan dan wawasan terkait implementasi laboratorium *cybersecurity* virtual menggunakan *Proxmox VE*.

didikan, dapat digunakan sebagai referensi dalam penggunaan si dalam bidang pendidikan dan praktikum *cybersecurity.*

kungan virtual yang aman dan terkontrol bagi mahasiswa Prodi untuk mempelajari dan mempraktikkan berbagai aspek

Optimized using
trial version
www.balesio.com

1.6 Landasan Teori

1.6.1 Laboratorium

Secara umum laboratorium memiliki beberapa indikator, laboratorium dapat didefinisikan sebagai sebuah ruangan atau bangunan untuk eksperimen, tes dan penelitian ilmiah, dengan makna ini, laboratorium dilihat sebagai perangkat keras. Dilihat sebagai perangkat lunak, laboratorium juga dapat diartikan sebagai sarana media untuk melakukan proses belajar dan mengajar atau sebagai pelengkap pembelajaran. Laboratorium juga dapat diartikan sebagai pusat berbagai kegiatan ilmiah untuk menemukan fakta kebenaran, tempat untuk menguji kebenaran ilmiah, sehingga laboratorium berfungsi sebagai barometer dalam keberhasilan pembelajaran (Riyadi, 2019).

1.6.2 Laboratorium Virtual

Laboratorium virtual adalah sekumpulan alat laboratorium yang berbasis perangkat lunak atau *software* yang dijalankan melalui komputer dan kegiatan di laboratorium dapat disimulasikan melalui komputer tersebut sehingga memberi pengguna kesan bahwa sedang berada di laboratorium yang sebenarnya. Laboratorium virtual dapat meningkatkan pengalaman belajar dan menjadikannya lebih efisien. Laboratorium virtual ini diharapkan dapat mengatasi masalah belajar dan mengurangi biaya pengadaan peralatan dan bahan praktikum (Kusumaningsih et al., 2014).

Ada beberapa keuntungan laboratorium virtual dibandingkan laboratorium fisik adalah penghematan biaya, laboratorium virtual menyediakan cara yang hemat bagi sekolah dan universitas untuk melakukan berbagai kegiatan penelitian khususnya dalam bidang sains, teknologi dan rekayasa. Dalam melakukan eksperimen, rekayasa dan simulasi dapat dibuat dengan mudah dengan biaya yang lebih rendah. Memungkinkan perubahan konfigurasi sistem dan perubahan parameter untuk melakukan pengujian dalam laboratorium virtual. Namun, ada beberapa keterbatasan pada laboratorium virtual yaitu bergantung pada kecepatan jaringan internet, kemudian kurangnya rasa tanggung jawab siswa karena merasa seperti bermain video *game*. Pada tahap akhir pelatihan pada laboratorium virtual biasanya tetap membutuhkan peralatan nyata untuk memperoleh keterampilan dengan pengalaman praktis (Potkonjak et al., 2016).

1.6.3 *Cybersecurity*

Konsep *cybersecurity* tidak memiliki definisi secara umum, namun *International Telecommunication Union* (ITU) mendefinisikan *cybersecurity* sebagai “kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber*, organisasi dan aset pengguna. *Cybersecurity* berusaha untuk memastikan pencapaian dan pemeliharaan properti dan aset pengguna terhadap risiko keamanan yang relevan di a” (itu.int, 2024). Tujuan *cybersecurity* adalah untuk memastikan nan aset dan pengguna suatu organisasi dapat dicapai dan dijaga ın *cyber*.

Optimized using
trial version
www.balesio.com

1.6.4 Virtualisasi

Virtualisasi adalah teknologi yang memungkinkan komputer dibagi menjadi beberapa lingkungan pada saat yang bersamaan. Lingkungan ini bisa saling terhubung atau bahkan tidak berhubungan sama sekali. Lingkungan ini sering disebut sebagai Virtual *Machine* (VM). Teknologi virtualisasi bertindak seolah-olah membuat komputer fisik menjadi ada dua atau lebih komputer logis, sehingga masing-masing komputer logis (non-fisik) memiliki arsitektur dasar yang sama dengan komputer fisik (Rusydi Umar, 2013). Virtualisasi merupakan metode untuk membuat sesuatu dalam bentuk virtual yang berbeda dari apa yang ada di dunia nyata. Dengan virtualisasi perangkat keras komputer dibuat seolah-olah tidak ada, atau bahkan membuat perangkat yang tidak ada menjadi ada. Dengan menggunakan virtualisasi, suatu perangkat keras dapat menjalankan beberapa sistem operasi dan layanan sekaligus, meningkatkan efisiensi penggunaan sumber daya, dan mengoptimalkan penggunaan lebih dari satu prosesor (Arfiandi, 2012).

Dalam jurnal yang ditulis oleh Arfiandi, (2012) mengemukakan ada 3 jenis pendekatan virtualisasi sebagai berikut:

1. *Partial Virtualisasiization*

Virtualisasi parsial merupakan bentuk virtualisasi hanya sebagian dari perangkat keras saja. Perangkat lunak virtualisasi parsial akan meniru, seolah-olah perangkat komputer memiliki alat tersebut.

2. *Full Virtualisasiization*

Virtualisasi penuh yaitu membuat seolah-olah ada sebuah komputer lain di dalam komputer. Misalnya dengan pemasangan *Linux* dalam *Windows*, demikian juga pemasangan *Windows* dalam *Linux.*

3. *Hardware-assisted Virtualisation*

Virtualisasi ini didukung oleh *hardware*. Jadi ada *hardware* khusus untuk meningkatkan *performance* proses *virtualisasi*. *Hardware-assisted* virtualisation mempunyai fitur *overheat*, sehingga performa *guest* OS tidak turun secara signifikan, maka dibantu dengan *hardware.*

Dalam jurnal yang ditulis oleh Xavier dkk., (2013) membahas ada 2 jenis virtualisasi yang umum digunakan yaitu:

1. Virtualisasi berbasis kontainer (*Container*-based *Virtualization*)

Virtualisasi ini bekerja pada tingkat sistem operasi, menciptakan beberapa ruang yang terisolasi. Setiap kontainer berbagi *kernel host* tetapi memiliki lingkungan yang terisolasi untuk menjalankan aplikasi. Kontainer ini lebih ringan daripada virtualisasi yang berbasis *hypervisor* karena tidak memerlukan *kernel* seperti Linux server, OpenVZ, Linux *Container*s (LXC). Virtualisasi ini menawarkan kinerja yang hampir sama dengan sistem operasi asli (*near-native performance*) dan cocok untuk lingkungan HCP (*High-Performance Computing*).

2. Virtualisasi berbasis *Hypervisor* (*Hypervisor-based Virtualization*)

ypervisor bekerja pada tingkat *hardware*, dengan hypervisor yang penuh dari mesin virtual. Setiap mesin virtual memiliki sistem erjalan sepenuhnya terisolasi dari yang lain. Meskipun lebih berat ontainer, virtualisasi berbasis *hypervisor* seperti Xen, Vmware, dan untuk menjalankan beberapa sistem operasi yang berbeda pada

Optimized using
trial version
www.balesio.com

1.6.5 Proxmox Virtual Environment

Proxmox Virtual Environment (PVE) adalah *hypervisor* berbasis *cluster* yang dapat digunakan untuk mengelola *virtual machine* dan mendukung *high availability* (Hariyadi & Juliansyah, 2018). Proxmox dibangun di atas *kernel* Linux yang berbasis Debian (64 bit) yang memungkinkan pengguna untuk membuat dan mengelola berbagai jenis lingkungan virtual, seperti mesin *virtual* (VM dan kontainer (CT). Dengan dukungan untuk teknologi *virtualisasi* seperti KVM (*Kernel*-based Virtual *Machine*) dan LXC (Linux *Container*s), *Proxmox* menawarkan kemampuan sistem dan fleksibilitas yang tinggi dalam membangun lingkungan *virtual* yang kompleks, pengaturan penyimpanan dan fungsi jaringan pada satu platform sehingga dengan mudah untuk mengelola *cluster*, *Proxmox* juga telah menyediakan alat pemulihan dan antarmuka manajemen web (Proxmox, 2024).

Proxmox merupakan solusi virtualisasi *open-source* yang memungkinkan pengguna untuk membuat banyak mesin virtual dan mengelolanya melalui antarmuka web. Dengan Proxmox pengguna dapat mengelola mesin virtual, penyimpanan, *node*, dan lainnya. Proxmox memungkinkan untuk memulai, menutup, menghapus dan melakukan migrasi mesin virtual (Chen et al., 2017).

Beberapa teknologi yang dapat digunakan pada Proxmox VE termasuk virtualisasi sistem operasi dan perangkat yaitu LXC, KVM, QEMU, HA dan Cluster Manager (Proxmox, 2024).

1. *Linux Container* (LXC)

LXC adalah teknologi virtualisasi yang memungkinkan menjalankan beberapa sistem operasi yang terisolasi dalam satu *kernel Linux*. Hal ini memungkinkan pengguna untuk menjalankan beberapa aplikasi atau layanan berbeda pada satu *server* atau komputer tanpa perlu memasang sistem operasi terpisah untuk setiap aplikasi

2. *Kernel* Virtual *Machine* (KVM)

KVM adalah modul *kernel* Linux yang mengubah *kernel* menjadi hypervisor, memanfaatkan ekstensi virtualisasi perangkat keras CPU untuk menyediakan virtualisasi penuh. Teknologi ini memungkinkan isolasi dan alokasi sumber daya yang efisien, memungkinkan beberapa mesin virtual berjalan secara bersamaan pada satu *host* fisik. KVM berperan penting dalam menyediakan lingkungan virtualisasi yang kuat dan efisien untuk menjalankan berbagai sistem operasi tamu.

3. *Quick Emulator* (QEMU)

QEMU adalah emulator dan virtualisasi mesin *open-source* yang dapat bekerja sebagai emulator penuh atau berkolaborasi dengan KVM. Dalam Proxmox, QEMU menyediakan emulasi perangkat keras virtual dan mendukung berbagai arsitektur CPU beserta perangkat. Kemampuannya meliputi emulasi CPU, memori dan perangkat I/O, serta mendukung fitur canggih seperti migrasi langsung (*live migration*) VM antar *host*.

HA)

tersediaan tinggi untuk VM dan kontainer, sistem ini memantau mendeteksi kegagalan, mendukung konfigurasi yang fleksibel dan me *fetching*. Fitur ini memungkinkan admin menentukan prioritas si untuk melakukan pengelolaan yang terperinci dalam *cluster*

5. *Cluster* Manager

Proxmox VE *Cluster Manager* (PVECM) merupakan teknologi yang memungkinkan untuk melakukan pengelompokan server fisik menjadi satu *cluster* untuk manajemen terpusat berbasis *web*. *Cluster* ini menggunakan *corosync* untuk komunikasi dan tidak memiliki batasan jumlah *node* tergantung dengan performa *hardware* yang digunakan. Dengan *cluster*, *admin* dengan mudah menambahkan atau menghapus *node*, dan mendapatkan manfaat dari fitur-fitur seperti manajemen *multi-master*, sinkronisasi konfigurasi *real-time* pada semua *node*, migrasi VM/*container* secara langsung, dan layanan *cluster-wide*.

1.6.6 Praktikum *Cybersecurity*

Cybersecurity didefinisikan sebagai perlindungan terhadap *cyberspace* itu sendiri, lingkungan virtual yang dibentuk oleh jaringan komputer termasuk internet, sistem informasi, dan infrastruktur teknologi informasi lainnya. *Cybersecurity* merupakan konsep yang luas yang melibatkan perlindungan terhadap berbagai aset, termasuk informasi, infrastruktur, individu, dan aset lainnya yang rentan terhadap serangan *cyber* (Von Solms & Van Niekerk, 2013).

Dalam jurnal yang ditulis oleh (Li & Liu, 2021), ada beberapa jenis *cybersecurity* yang perlu dipahami yaitu:

1. Keamanan jaringan (*Network Security*) merupakan serangkaian solusi yang bertujuan untuk melindungi jaringan komputer dari serangan berupa *malware* atau peretasan. Contohnya seperti *firewall*, VPN dan lain-lain.
2. Keamanan Aplikasi (*Application Security*) yaitu menggunakan perangkat keras dan perangkat lunak bertujuan untuk melindungi sistem dari ancaman eksternal yang dapat mengganggu pengembangan aplikasi. Contohnya seperti program antivirus, enkripsi dan *firewal*l.
3. Keamanan Informasi (*Information Security*) yaitu melindungi data fisik dan data digital dari penyalahgunaan, akses, perubahan dan penghapusan yang tidak sah.
4. Keamanan Operasional (*Operational Security*) yaitu proses dan keputusan yang dibuat untuk mengontrol dan melindungi data. Misalnya, izin pengguna saat mengakses jaringan atau proses yang menentukan kapan dan di mana informasi dapat disimpan atau dibagikan.
5. Keamanan *Cloud* yaitu melindungi informasi di *cloud*, dan memantau untuk mengantisipasi risiko serangan data pada *cloud*.
6. Pelatihan Pengguna yaitu mengacu pada aspek *cybersecurity* yang tidak dapat diprediksi, yaitu individu. Siapa pun dapat terkena serangan virus dengan tidak sengaja masuk ke dalam komputer. Mengajari pengguna untuk menghapus lampiran yang mencurigakan di *e-mail*, tidak menggunakan USB yang tidak dikenal, dan masalah kritis lainnya.

gkat Lunak (*Software Security*) yaitu teknologi untuk melindungi dari serangan, kerentanan, dan eksploitasi yang dapat stem dan data yang diolah oleh perangkat lunak.

ecurity memiliki peran penting dalam menjaga keamanan dan nasi, serta melindungi data dari ancaman *cyber* yang beragam. Li & n bahwa ada beberapa jenis serangan *cyber* yaitu:

Optimized using
trial version
www.balesio.com

1. *Denial of Service* (DoS); serangan DoS bertujuan untuk membuat layanan atau sumber daya tidak tersedia lagi bagi pengguna yang sah dengan membanjiri sistem atau jaringan dengan lalu lintas data yang berlebihan, sehingga mengganggu ketersediaan layanan.
2. *Logical Bomb*; serangan ini melibatkan penyisipan kode ke dalam program yang akan melakukan aktivitas merusak secara otomatis jika suatu kondisi terpenuhi, yang dapat menyebabkan kerusakan pada sistem.
3. *Abuse Tools*; serangan ini menggunakan alat-alat yang tersedia untuk mendeteksi dan memanfaatkan kerentanan dalam jaringan dengan berbagai tingkat keterampilan, sehingga memungkinkan penyerang untuk masuk ke dalam sistem target.
4. *Sniffer*; merupakan program yang digunakan untuk mengintai informasi yang dikirim melalui jaringan dengan tujuan mencuri data sensitif seperti kata sandi dengan menganalisis paket data yang dikirim.
5. *Trojan Horse*; Jenis serangan di mana perangkat lunak berbahaya disamarkan sebagai program yang berguna atau aman untuk mengelabui pengguna agar mengunduhnya, yang kemudian dapat digunakan untuk merusak sistem.
6. *Virus dan worm*; Virus adalah program yang dapat menginfeksi berkas dalam komputer dan mereplikasi dirinya sendiri, sementara *worm* adalah program mandiri yang dapat menyebar ke komputer lain melalui jaringan.
7. *Spam*; Serangan spam melibatkan pengiriman pesan yang tidak diinginkan kepada pengguna dengan tujuan mengganggu atau membanjiri kotak *masuk e-mail* mereka.
8. *Botnet*; Merupakan jaringan komputer yang terinfeksi oleh *malware* dan dikendalikan oleh penyerang secara *remote* untuk melakukan serangan koordinasi, seperti DdoS.

Pemahaman tentang berbagai jenis *cybersecurity* dan serangan *cyber* tersebut, individu dan organisasi dapat meningkatkan kewaspadaan terhadap ancaman *cyber* dan mengambil langkah-langkah perlindungan yang sesuai untuk melindungi sistem dan data.

1.6.7 Technology Acceptance Model (TAM)

Technology Acceptance Model (TAM) adalah model penelitian yang dikembangkan oleh Davis pada tahun 1985 untuk menganalisis faktor-faktor yang mempengaruhi penerimaan teknologi komputer. TAM merupakan model yang dimodifikasi dari *Theory of Reasoned Action* (TRA) yang dikembangkan oleh Fishbein dan Ajzen, dimana nilai utamanya adalah persepsi kegunaan dan kemudahan. Persepsi kegunaan untuk melihat seberapa jauh orang yakin dalam menggunakan suatu sistem agar memaksimalkan kinerja. Persepsi kemudahan untuk melihat sejauh mana orang yakin tentang sebuah sistem yang mudah digunakan (Pratama et al., 2022)

1.6.8 Penelitian Terkait

Berikut adalah penelitian terkait yang dilakukan menggunakan virtualisasi

Tabel 1. Penelitian Terkait

1	Peneliti	Hendi Suhendi, Indra Nurdiyana
	Tahun Penelitian	2017
	Judul Penelitian	"Manajemen Server Jaringan Komputer Berbasis Teknologi Virtualisasi Menggunakan Proxmox"
	Hasil Penelitian	Penelitian ini membuktikan bahwa penggunaan Proxmox sebagai teknologi virtualisasi mampu menggantikan dua server fisik dengan sumber daya terbatas menjadi satu server berkinerja tinggi. Hasilnya menunjukkan pengurangan ketergantungan pada *hardware* fisik, kemudahan *maintenance*, serta peningkatan efisiensi penyimpanan dan berbagi data. Selain itu, teknologi ini menghemat waktu, menurunkan biaya operasional, dan mengoptimalkan penggunaan sumber daya server. Penelitian menyimpulkan bahwa Proxmox efektif untuk infrastruktur IT yang membutuhkan kinerja sistem dan fleksibilitas tanpa investasi *hardware* besar.
2	Peneliti	Edwar Ali, Susandri, Rahmaddeni
	Tahun Penelitian	2015
	Judul Penelitian	"*Optimizing Server Resource by Using Virtualization Technology*"
	Hasil Penelitian	Melalui observasi selama 15 hari pada 7 server virtual dan 3 server fisik, penelitian ini menemukan bahwa virtualisasi meningkatkan efisiensi penggunaan CPU, memori, dan *bandwidth* jaringan. Server virtual terbukti mampu menangani beban kerja yang sebelumnya memerlukan lebih banyak server fisik, sehingga mengurangi biaya pembelian dan operasional server baru. Kesimpulan penelitian menegaskan bahwa virtualisasi tidak hanya mengoptimalkan sumber daya, tetapi juga meningkatkan keandalan sistem dan mempercepat pemulihan data melalui fitur *snapshot* Proxmox.

Optimized using
trial version
www.balesio.com

3	Peneliti	Abdurrahman, Soni, Afdhil Hafid
	Tahun Penelitian	2019
	Judul Penelitian	"Optimalisasi Sumber Daya Komputer dengan Virtualisasi Server Menggunakan Proxmox VE"
	Hasil Penelitian	Penelitian ini menguji efektivitas Proxmox VE dalam mengoptimalkan sumber daya komputer. Hasil eksperimen menunjukkan peningkatan efisiensi penggunaan CPU hingga 30% dan memori hingga 25% dibandingkan server fisik. Selain itu, Proxmox VE memudahkan manajemen server terpusat dan menyederhanakan proses *backup*/replikasi data. Peneliti menyarankan peningkatan integrasi teknologi virtualisasi untuk meningkatkan keamanan jaringan dan skalabilitas sistem, terutama bagi organisasi yang ingin beralih ke infrastruktur *hybrid* dengan biaya minimal.

Beberapa penelitian sebelumnya menunjukkan bahwa teknologi virtualisasi dapat meningkatkan efisiensi pengelolaan server dan infrastruktur jaringan. Menurut penelitian yang dilakukan oleh Hendi Suhendi dan Indra Nurdiyana (2017), Proxmox dapat menggunakan satu server virtual dengan lebih sedikit pengelolaan dan penggunaan sumber daya. Selain itu, penelitian yang dilakukan oleh Edwar Ali, Susandri, dan Rahmaddeni (2015) menekankan bahwa virtualisasi memiliki kemampuan untuk mengurangi biaya operasional dengan mengoptimalkan CPU, *memori*, dan *bandwidth* jaringan. Sementara itu, penelitian yang dilakukan pada tahun 2019 oleh Abdurrahman, Soni, dan Afdhil Hafid menunjukkan bahwa Proxmox VE meningkatkan efisiensi hingga 30% dan membuat manajemen server lebih mudah. Hasilnya akan mendorong penelitian ini untuk menggunakan Proxmox VE untuk optimalisasi sumber daya dan untuk menggunakannya sebagai media pembelajaran praktikum *cybersecurity* dengan menggunakan platform seperti DVWA dan Metasploitable.

1.7 Kaitan Dengan Sistem Informasi

Menurut Barata dan Cunha (2013), sistem informasi tidak hanya terdiri dari perangkat keras dan perangkat lunak semata, melainkan merupakan suatu sistem yang saling terkait dimana melibatkan lima dimensi utama, yaitu *Contecxt*, *People*, *Process*, IT, dan

am dimensi *context* mencakup faktor *eksternal* dan kebijakan engaruhi system, dimensi *people* mengacu pada pengguna dan an yang terlibat secara langsung, dimensi *process* merupakan ur kerja yang didukung oleh system, dimensi IT mencakup i seperti *hardware, software* dan jaringan, serta dimensi cakup data yang dikumpulkan dan diolah untuk mendukung an.

Penerapan sistem informasi manajemen dalam institusi pendidikan berperan penting dalam meningkatkan efesiensi pelatihan, dan responsif terhadap tuntutan local (Shniekat et al., 2022). Sistem informasi tidak hanya menyelesaikan masalah teknologi, tetapi juga dalam pemberdayaan manusia dan efesiensi dalam proses pembelajaran. Dalam konteks penelitian ini, pengembangan laboratorium virtual berbasis Proxmox menjadi contoh dalam penerapan berbagai dimensi dalam sistem informasi seperti infrastruktur Proxmox sebagai teknologi virtualisasi, aspek *people* (pengguna), *process* (praktikum *cybersecurity*, dan *data* (hasil evaluasi TAM).

Optimized using
trial version
www.balesio.com

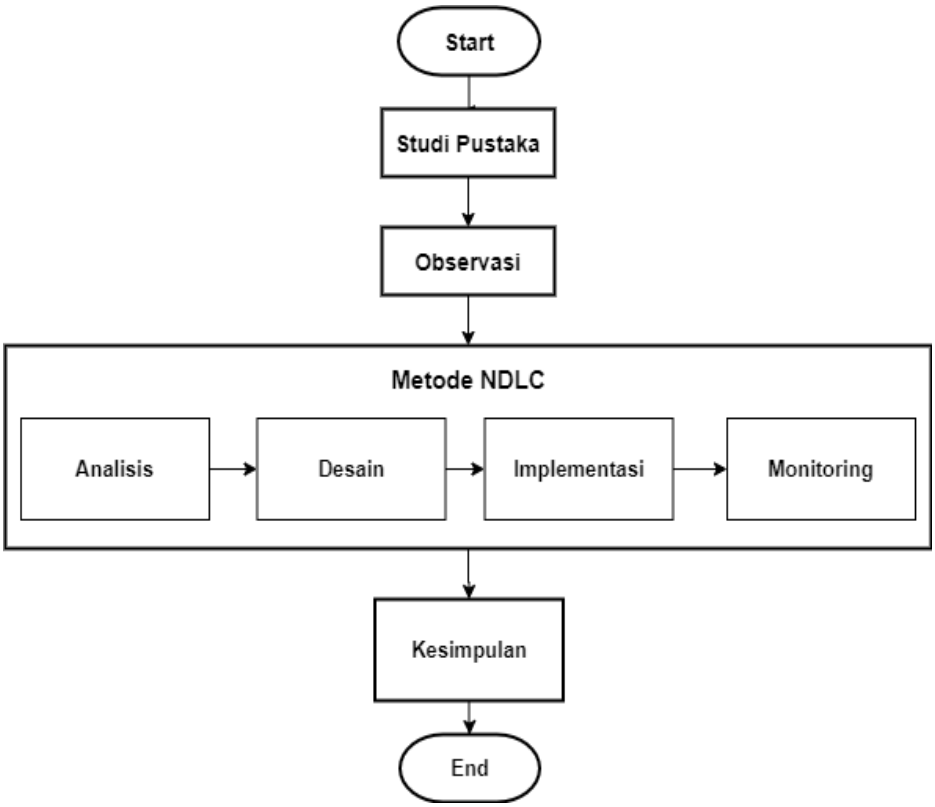
BAB II
METODE PENELITIAN

2.1 Waktu dan Lokasi Penelitian

Penelitian ini dilaksanakan di Laboratorium Komputer Prodi Sistem Informasi Universitas Hasanuddin, dengan waktu pelaksanaan mulai bulan Agustus 2024 hingga Maret 2025. Lokasi ini dipilih karena memiliki fasilitas yang memadai untuk mendukung implementasi laboratorium *cybersecurity* virtual.

2.2 Tahapan Penelitian

Tahapan penelitian mencakup langkah-langkah pelaksanaan dari pertama hingga terakhir, tahapan pada penelitian ini sebagaimana ditunjukkan pada Gambar 1.



Gambar 1. Bagan alir tahapan penelitian

2.3 Instrumen Penelitian

ang digunakan pada penelitian ini terbagi dua yaitu instrumen *ware*) dan instrumen perangkat lunak (*Software*).

digunakan adalah komputer dengan spesifikasi sebagai berikut:
Intel i5-12400F (12) 4.4GHz

Optimized using
trial version
www.balesio.com

3. Kapasitas penyimpanan 512 GB

b. Perangkat Lunak
Perangkat lunak yang digunakan dalam penelitian ini mencakup:

1. Proxmox Virtual Environment
2. Sistem Operasi Linux Ubuntu
3. Docker
4. Influx DB
5. Grafana
6. Draw.io

2.4 Teknik Pengumpulan Data
Teknik yang dilakukan untuk mengumpulkan data adalah sebagai berikut:

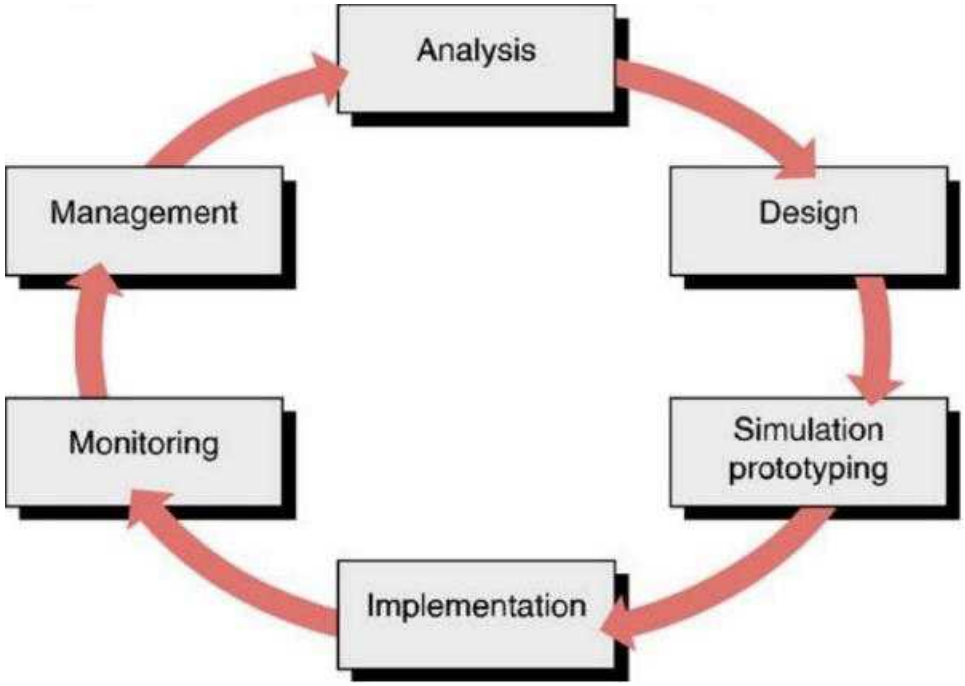
2.4.1 Studi Pustaka
Studi pustaka diawali dengan mencari informasi dari berbagai sumber, termasuk buku, jurnal, dan artikel yang berkaitan dengan teknologi virtualisasi Proxmox VE dan aspek *cybersecurity*. Proses ini dilakukan untuk mendapatkan pemahaman, ide-ide, dan teknologi yang digunakan. Studi pustaka juga bertujuan untuk menemukan penelitian sebelumnya yang dapat digunakan sebagai landasan teori untuk pengembangan dan analisis sistem yang dikaji. Oleh karena itu, informasi yang dikumpulkan dari berbagai literatur ini akan membantu dalam menciptakan penyelesaian yang berguna serta memperkuat teori yang mendukung penelitian ini.

2.4.2 Observasi
Penulis melakukan observasi pada Laboratorium Komputer Prodi Sistem Informasi Universitas Hasanuddin dengan maksud agar penulis dapat lebih memahami situasi dan mengetahui sumber daya pada Laboratorium Prodi tersebut yang sedang digunakan.

2.4.3 Memonitor Kerja
Pengumpulan data kinerja menggunakan Proxmox VE *Metrics Server*, yang memungkinkan untuk mengumpulkan informasi tentang penggunaan sumber daya secara *real-time*. Data yang dikumpulkan mencakup penggunaan CPU, penggunaan memori, aktivitas *disk* dan aktivitas jaringan.

2.5 Metode NDLC
Metode *Network Development Life Cycle* (NDLC) digunakan dalam mengembangkan atau merancang jaringan infrastruktur dan memungkinkan pemantauan dan pengelolaan jaringan. NDLC dibagi menjadi enam tahap yaitu analisis, desain, *...pe*, implementasi, pemantauan, dan manajemen (Rianafirin &

Optimized using
trial version
www.balesio.com



Gambar 2. *Network Development Life Cycle (NDLC)*

Sumber: (Kosasi, 2011)

Pada Gambar 2 menunjukkan metode NDLC yang menggambarkan setiap tahapan atau mekanisme suatu cara dengan saling terhubung. Pada metode NDLC, semua tahapan dan proses pengembangan jaringan yang bersambung-sambung seperti *cycle*. Dalam penelitian ini, ada lima tahapan yang digunakan dalam penelitian ini yaitu:

2.5.1 Analisis

Tahapan awal penelitian yaitu melakukan analisis terhadap instrumen penelitian pada Prodi Sistem Informasi agar konfigurasi dan kebutuhan perangkat lunak dapat disesuaikan sesuai kebutuhan.

a. Perangkat keras yang digunakan dalam penelitian ini adalah:
   - Mikrotik GX
   - Komputer yang digunakan ditunjukkan pada Tabel 1 Spesifikasi Komputer pada Prodi Sistem Informasi

Optimized using
trial version
www.balesio.com

Tabel 2. Spesifikasi komputer *host*

Parameter	Nilai
Prosesor	*Intel Core* i5-12400F
RAM	16 GB
Disk Penyimpanan	512 GB

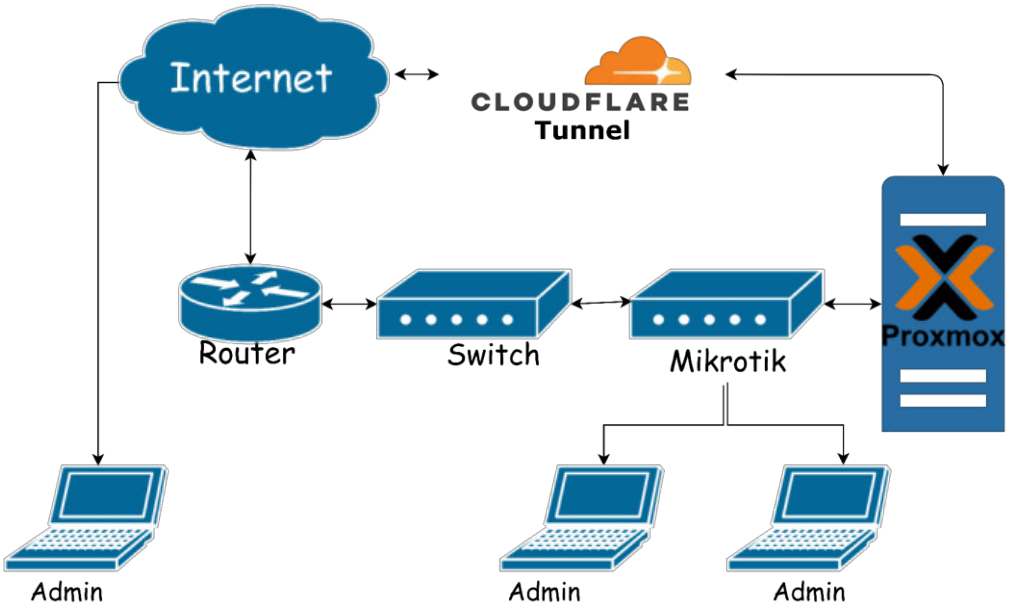
c. Perangkat lunak yang digunakan untuk pengujian pada penelitian ini sebagai berikut:
   - Proxmox VE versi 8.3.2
   - Draw.io
   - Portainer
   - Grafana
   - InfluxDB
   - Cloudflare
   - ZeroTier
   - MkDocs

d. Jaringan meliputi *switch hub* dan mikrotik yang terhubung ke Proxmox, konfigurasi *bridge interface* pada Proxmox juga dilakukan untuk mendukung konektivitas VM dan akses ke jaringan lokal Proxmox.

2.5.2 Desain

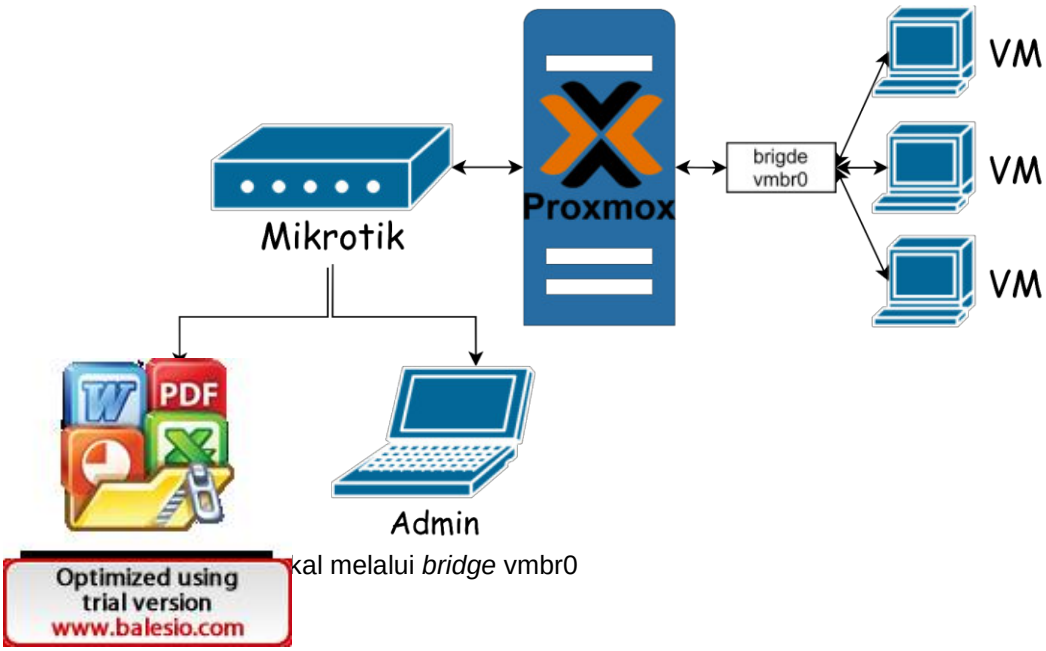
a. Struktur Jaringan

Tahapan kedua dari penelitian ini adalah desain. Tujuan dari tahap ini adalah untuk mengetahui bagaimana gambaran sistem akan bekerja. Struktur jaringan dikonfigurasi untuk menghubungkan *node* Proxmox VE ke jaringan lokal melalui LAN dan internet.



Gambar 3. Struktur jaringan

Struktur jaringan yang digunakan dalam laboratorium virtual ini mengadopsi konsep jaringan terpusat, sehingga semua komponen Proxmox, mikrotik dan komputer admin dapat saling terhubung dalam satu jaringan yang saling berhubungan melalui *routing lan* dan *tunneling*. Proxmox VE yang menjalankan VM menggunakan jaringan *bridge* virtual vmbr0 untuk menjembatani VM ke jaringan lan, sehingga semua komunikasi jaringan antar VM dengan perangkat eksternal dilakukan melalui *bridge* ini. Setiap VM diberi alamat IP melalui vmbr0 dengan IP segmen yang sama digunakan oleh *host*.



kal melalui *bridge* vmbr0

Optimized using
trial version
www.balesio.com

Router berfungsi sebagai penghubung antara Proxmox dan internet, *router* mengelola alokasi IP bagi perangkat yang terhubung termasuk pada *switch*. Pengaturan *firewall* dasar pada *router* memastikan keamanan data selama transmisi. Mikrotik dalam struktur rangkaian jaringan ini berfungsi sebagai penghubung antara admin dengan Proxmox, mikrotik juga digunakan untuk mengisolasi jaringan dengan cara memberikan alamat IP menggunakan *gateway* yang beda dari *router* agar tidak mempengaruhi *router* utama.

b. Struktur Sistem

Laboratorium *cybersecurity* virtual yang diimplementasikan dalam penelitian ini dibangun dengan menggunakan Proxmox VE sebagai platform virtualisasi utama. Arsitektur sistem ini bertujuan untuk menyediakan lingkungan yang fleksibel dan aman untuk melakukan berbagai skenario pembelajaran dan pengujian *cybersecurity*. Arsitektur laboratorium *cybersecurity* virtual yang diimplementasikan terdiri dari satu komputer fisik Proxmox VE yang mengelola beberapa virtual *machine* (VM). Komputer ini terhubung ke jaringan melalui Mikrotik sehingga memungkinkan manajemen jaringan, alamat IP dan akses *remote* bagi pengguna.

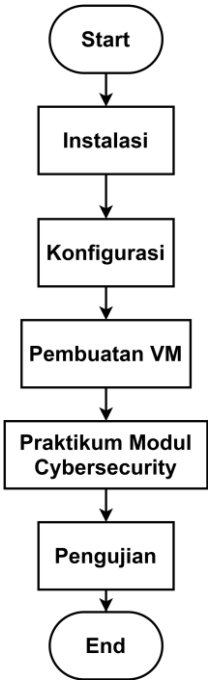
Setiap *Virtual Machin*e yang dipasang dalam Proxmox dikonfigurasi untuk menjalankan peran spesifik dalam skenario keamanan seperti VM untuk melakukan pengujian *resource*, VM untuk simulasi melakukan serangan seperti menggunakan VM Kali Linux dan *Metasploitable*2 yang berisi DVWA. Semua VM ini terhubung melalui jaringan virtual yang dikonfigurasi dalam Proxmox VE. Konfigurasi jaringan virtual ini memungkinkan lab untuk terisolasi dari jaringan fisik sumber internet Proxmox VE menggunakan *bridge* jaringan virtual (vmbr0) yang terhubung langsung ke *router* melalui mikrotik yang berfungsi sebagai *gateway* utama dan *firewall*. Melalui *bridge* virtual, setiap mesin virtual dalam Proxmox menerima alamat IP dengan segmen yang sama, sehingga memungkinkan VM dapat berinteraksi satu sama lain dan mengakses sumber daya jaringan.

Manajemen laboratorium virtual ini dilakukan melalui *web interface* Proxmox VE yang dapat diakses secara aman dari jaringan lokal maupun dari luar jaringan lokal. *Interface* ini memungkinkan administrator dengan mudah membuat, mengkonfigurasi, dan mengelola VM, serta memantau sumber daya sistem.

Dengan arsitektur seperti ini, laboratorium *cybersecurity* virtual dapat mendukung berbagai skenario praktikum pembelajaran. Fleksibilitas arsitektur ini juga memungkinkan penambahan atau modifikasi komponen di masa depan sesuai dengan perkembangan kebutuhan laboratorium dan pembelajaran di bidang *cybersecurity*.

2.5.3 Implementasi

Implementasi dalam perancangan laboratorium virtual *cybersecurity* ini, yaitu pembuatan *Virtual Machine*, modul praktikum dan pengujian.



Gambar 5. Implementasi dalam perancangan laboratorium virtual

Berdasarkan Gambar 5, implementasi dalam perancangan laboratorium virtual *cybersecurity* dapat dijelaskan sebagai berikut:

a. Instalasi

Tahapan instalasi dilakukan dengan pemasangan perangkat lunak Proxmox yang berfungsi sebagai sistem operasi utama dalam komputer. Setelah itu pengalamatan IP juga menjadi bagian penting agar komputer mendapat alamat IP dan sumber internet. Seluruh proses instalasi dilakukan dengan benar agar seluruh fitur dan fungsi berjalan sesuai dengan kebutuhan. Setelah instalasi Proxmox VE selesai maka langkah selanjutnya adalah memastikan bahwa sistem telah diperbaharui ke versi terbaru untuk memastikan stabilitas dan keamanan.

b. Konfigurasi

Setelah melakukan penginstalan maka tahapan selanjutnya yaitu melakukan konfigurasi. Konfigurasi jaringan dasar dilakukan seperti membuat jaringan *virtual bridge* (*vmbr0*) untuk menghubungkan *node* Proxmox ke jaringan lokal (LAN). Konfigurasi Metrik Server juga perlu dilakukan agar bisa terhubung data *resource* bisa disimpan dan ditampilkan melalui InfluxDB dan Grafana.

Optimized using
trial version
www.balesio.com

Machine **(VM)**

tual *Machine* (VM) di *Proxmox* merupakan langkah penting dalam lingkungan virtualisasi. VM memungkinkan sistem operasi dan n wadah terisolasi, Proses konfigurasi VM di *Proxmox* dilakukan yang dibutuhkan, kemudian penentuan alokasi memori dan sumber ta konfigurasi pengalamatan IP.

Proxmox VE memiliki akses penuh kepada VM tersebut, melalui antarmuka grafis yang dimiliki *Proxmox* dapat melakukan pembuatan, atau penghapusan sebuah VM. Kemampuan untuk memantau, mengelola dan mengoptimalkan kinerja VM secara *real-time* dapat dilakukan oleh Proxmox untuk memastikan efisiensi penggunaan VM.

Untuk membuat VM, administrator harus memiliki *file* tunggal sebuah operasi sistem (ISO) kemudian diunggah ke dalam Proxmox. Administrator harus menetapkan parameter penting dalam pembuatan VM pada Proxmox seperti pemilihan sistem operasi yang sesuai dan menentukan kapasitas memori, jumlah unit pemrosesan, dan ruang penyimpanan yang dibutuhkan. Setelah konfigurasi selesai dan VM berhasil dibuat, antarmuka grafis Proxmox VE digunakan untuk mengatur dan mengawasi kinerja VM tersebut.

Proxmox mampu menjalankan banyak aplikasi atau sistem operasi secara terpisah dalam satu infrastruktur fisik, metode ini memiliki beberapa keuntungan yaitu:

1. Mengoptimalkan penggunaan sumber daya perangkat keras yang sudah ada.
2. Mengurangi biaya dalam pengadaan perangkat baru.
3. Meningkatkan fleksibilitas dan kemampuan skala sistem secara keseluruhan.

d. Konfigurasi modul dan Praktikum Modul *Cybersecurity*

Konfigurasi dan persiapan modul praktikum *cybersecurity* merupakan langkah penting dalam pengembangan laboratorium virtual. Berbagai elemen *cybersecurity* dan pengujian penetrasi dirancang dan diimplementasikan ke dalam lingkungan Proxmox VE. Setiap modul diatur dengan bertahap untuk memenuhi tujuan pembelajaran dan mengikuti perkembangan teknologi saat ini.

Memasang dan mengonfigurasi *Metasploitable*2 pada VM untuk melakukan simulasi dan menguji berbagai serangan keamanan seperti *brute force* menggunakan *tool Burp Suite* yang berjalan dalam VM Kali Linux.

e. Pengujian

Pengujian dalam penelitian ini dilakukan untuk memastikan bahwa sistem laboratorium virtual berbasis Proxmox VE berfungsi dengan optimal dalam mendukung pembelajaran *cybersecurity*. Metode pengujian yang digunakan mencakup dua pendekatan utama, yaitu pengujian teknis dan evaluasi berbasis *Technology Acceptance Model* (TAM) dengan metode penelitian kualitatif.

Pada pengujian teknis, dilakukan uji beban untuk mengukur kemampuan sistem dalam menangani sejumlah VM secara bersamaan. Uji ini dilakukan dengan membuat VM bertahap hingga mencapai batas maksimal sumber daya yang tersedia. VM uji dengan Ubuntu Server dikonfigurasi untuk menjalankan *stress testing* guna mengukur konsumsi CPU dan RAM pada Proxmox, sedangkan VM uji dengan Ubuntu Desktop digunakan untuk mengamati dampak sistem operasi berbasis grafik terhadap performa Proxmox. [illegible] meliputi kinerja CPU, penggunaan RAM, dan *delay* dalam

[illegible]eknis, evaluasi sistem juga dilakukan menggunakan pendekatan [illegible]ui tingkat penerimaan pengguna terhadap laboratorium virtual ini. [illegible]itatif digunakan dengan wawancara kepada responden yang terdiri [illegible]osen yang telah menggunakan laboratorium virtual dalam praktikum

Optimized using
trial version
www.balesio.com

2.5.4 *Monitoring*

Monitoring merupakan proses penting dalam pengelolaan laboratorium *cybersecurity* virtual menggunakan Proxmox. Sistem *monitoring* memungkinkan administrator untuk mengevaluasi kinerja dan penggunaan sumber daya secara menyeluruh. Untuk pengumpulan data numerik dalam implementasi ini, Proxmox VE Metrics Server dikonfigurasi untuk mengirimkan data *real-time* dari *node* Proxmox ke InfluxDB yaitu sebuah *database* yang dirancang untuk menyimpan data metrik. Data yang dikumpulkan mencakup informasi seperti penggunaan CPU, pemakaian memori, aktivitas *disk*, aktivitas jaringan, dan *delay*.

InfluxDB berfungsi sebagai penyimpanan utama untuk semua data metrik ini. Sistem pemantauan dilakukan dengan menggunakan Grafana. Grafana merupakan sebuah alat visualisasi yang dapat digunakan untuk menampilkan *dashboard* dari data yang tersimpan dari InfluxDB.

2.5.5 Kesimpulan

Pada tahap ini, ditarik kesimpulan tentang performa laboratorium *cybersecurity* virtual dapat digunakan dengan baik sehingga dapat memberikan manfaat dalam proses pembelajaran baik dalam Prodi Sistem Informasi maupun di luar lingkungan kampus.

2.6 Indikator Penilaian dengan Metode *Technology Acceptance Model* (TAM)

Indikator penilaian yang terdiri dari empat variabel tentang model survei digunakan untuk menentukan jumlah pernyataan yang dimasukkan dalam kuesioner. Berikut indikator penilaian yang digunakan:

Tabel 3. Indikator penilaian

No.	*Variable*	*Indicator*
1.	*Perceived Ease of Use* (PE)	Mudah dipahami
		Kemudahan dalam penggunaan
2.	*Perceived Usefulness* (PU)	Membantu pemahaman konsep
		Efisiensi waktu dan fleksibilitas
3.	*Attitude Toward Using* (ATU)	Ketertarikan terhadap penggunaan
		Keinginan untuk merekomendasikan
	ention to Use (BIU)	Niat untuk terus menggunakan
		Preferensi penggunaan

Optimized using
trial version
www.balesio.com