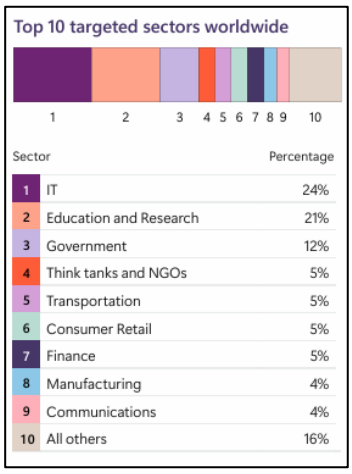
BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Serangan siber pada server sering kali menjadi sasaran utama dalam serangan fisik, ini menjadi sebuah propaganda konflik modern yang terjadi saat ini. Infrastruktur penting seperti server yang menyimpan data vital, sering kali memiliki celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Berdasarkan laporan pertahanan digital yang dilakukan oleh Microsoft (2024), pada akhir tahun 2023 masalah ini semakin menonjol karena banyak sistem infrastruktur kritis yang memiliki kelemahan serius dalam hal keamanan. Salah satu penyebabnya adalah perangkat yang tidak diperbarui dengan *patch* atau pembaruan keamanan terkini, membuatnya rentan terhadap eksploitasi oleh peretas. Selain itu, penggunaan kata sandi *default* yang mudah ditebak atau bahkan ketidakhadiran kata sandi sama sekali menjadi titik masuk yang potensial bagi penyerang untuk mengakses sistem tanpa hambatan berarti. Dalam era digital yang berkembang secara signikfikan, serangan yang mencakup kombinasi antara serangan fisik dan siber ini membuka peluang bagi pihak yang tidak bertanggung jawab untuk menyusup ke infrastruktur penting dan memanfaatkannya untuk tujuan sabotase, spionase, atau memanfaatkan data penting lainnya. (Microsoft, 2024).

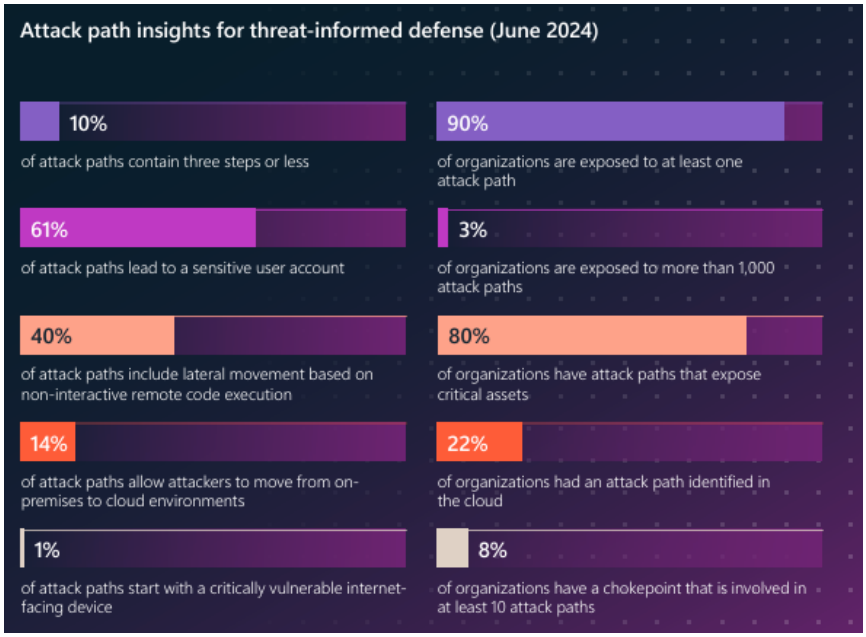


Gambar 1.1 Top 10 Sektor Target Serangan Siber

(Microsoft, 2024)

Berdasarkan Gambar 1.1 dikutip dari Microsoft Digital Defense 2024, melaporkan beberapa sektor target yang menjadi serangan siber. Diantaranya adalah teknologi informasi (IT) menjadi target utama dengan persentase sebesar 24%, diikuti oleh sektor pendidikan dan penelitian yang mencapai 21%. Pemerintahan juga termasuk dalam kategori yang rentan terhadap serangan dengan persentase 12%, mengindikasikan bahwa data sensitif dan informasi strategis dalam sektor ini menarik bagi pelaku ancaman. Secara keseluruhan, data ini mengindikasikan bahwa sektor-sektor yang memiliki nilai ekonomi dan strategis tinggi menjadi sasaran utama serangan, menegaskan pentingnya peningkatan langkah-langkah keamanan di berbagai industri. (Microsoft, 2024).

Peningkatan keamanan siber di sektor vital seperti pemerintahan dan perbankan menjadi krusial mengingat tingginya risiko serangan siber yang dapat mengancam stabilitas nasional dan kepercayaan publik. Sistem pemerintahan menyimpan data sensitif terkait kebijakan, keamanan negara, serta informasi pribadi warga negara, sementara sektor perbankan mengelola transaksi keuangan dalam jumlah besar yang rentan terhadap pencurian data dan penipuan siber. Serangan terhadap kedua sektor ini, seperti peretasan, ransomware, atau pencurian identitas, dapat menimbulkan dampak yang luas, mulai dari gangguan layanan publik hingga kerugian ekonomi yang signifikan penerapan langkah-langkah mitigasi yang komprehensif, seperti peningkatan enkripsi data, penggunaan autentikasi berlapis, serta pemantauan ancaman, menjadi sangat penting untuk memastikan ketahanan sistem terhadap ancaman siber yang semakin canggih dan kompleks. (Wibisono Gunawan dkk., 2024).



Gambar 1.2 *Insight* Upaya Serangan Siber

(Microsoft, 2024)

Gambar 1.2 menjelaskan beberapa upaya yang dilakukan untuk mencari kerentanan serangan siber. Dari sisi statistik, analisis jalur serangan menunjukkan bahwa 90% organisasi terpapar setidaknya satu jalur serangan, yang menandakan bahwa hampir semua organisasi memiliki titik lemah dalam sistem keamanannya.. Selain itu, 40% jalur serangan mencakup *lateral movement based* pada RCE (*Remote Code Execution*), yang memungkinkan penyerang berpindah dari satu sistem ke sistem lain tanpa terdeteksi, meningkatkan kompleksitas dalam mitigasi ancaman. Dikutip dari *insight* serangan siber pada gambar 1.2 adanya serangan *movement based* dapat disebut karena adanya virtualisasi. Menurut Maine Bahasa (2023) virtualisasi adalah teknologi yang memungkinkan satu server fisik untuk menjalankan beberapa mesin virtual secara bersamaan dengan menggunakan perangkat lunak. Teknologi ini membagi sumber daya fisik server, seperti CPU, RAM, dan penyimpanan, untuk digunakan secara efisien oleh berbagai lingkungan virtual yang terisolasi. Disamping keuntungan nya yang dapat menggunakan satu sumber daya secara berbagi dalam sistem yang terisolasi, atau dengan istilah *multi-tenancy*, dampak buruknya adalah potensi kebocoran data akibat kelemahan dalam isolasi antar tenant. Jika sistem keamanan tidak dirancang dengan baik, seorang

tenant yang tidak berwenang dapat mengakses data milik tenant lain, baik karena kesalahan konfigurasi, eksploitasi kelemahan sistem, atau serangan yang berhasil membobol batas isolasi yang ada. Kesalahan dalam manajemen akses atau kerentanan dalam mekanisme otorisasi dapat menyebabkan data yang seharusnya eksklusif menjadi terekspos ke pengguna lain dalam lingkungan yang sama. Selain kebocoran data, peretasan dalam *multi-tenancy* memiliki dampak yang lebih luas dibandingkan dengan sistem yang terisolasi secara penuh. Jika seorang *threat actor* berhasil mengeksploitasi celah keamanan dalam sistem yang digunakan bersama, mereka dapat memperluas serangan ke banyak tenant sekaligus. Serangan seperti *privilege escalation*, *injection attack*, atau *exploitation of shared resources* dapat memungkinkan penyerang mengakses informasi sensitif dari berbagai organisasi dalam satu infrastruktur.

Salah satu mitigasi yang dilakukan oleh Badan Siber dan Sandi Negara yaitu merilis imbauan keamanan siber berdasarkan acuan CVE (*Common Vulnerabilities and Exposures*), CVE adalah sistem klasifikasi yang digunakan secara global untuk mendokumentasikan berbagai kerentanan keamanan informasi yang ditemukan pada perangkat lunak, sistem operasi, atau perangkat keras. Setiap kerentanan yang terdaftar dalam CVE diberikan nomor identifikasi unik, deskripsi rinci mengenai kelemahan yang ditemukan, serta informasi mengenai potensi dampaknya. Sebagai contoh CVE-2023-20198 memiliki nilai CVSS 10.00 dengan dampak critical dampak dari kode CVE ini Jika kerentanan ini berhasil dieksploitasi, penyerang siber yang tidak sah dapat memanfaatkan *privilege escalation* untuk meningkatkan hak akses mereka dan membuat akun baru dengan hak administrator penuh. Dengan hak istimewa ini, mereka dapat mengendalikan sistem secara menyeluruh, termasuk mengubah konfigurasi keamanan, mengakses data sensitif, atau menginstal perangkat lunak berbahaya. (Badan Siber dan Sandi Negara, 2023).

Selain mitigasi dengan memberikan penyuluhan informasi pencegahan, perlu juga diupayakan langkah teknis dalam konsep pencegahan serangan siber pada server yang berbasis virtualisasi adalah dengan kontainerisasi, menurut (Adhikari & Baidya, 2024) kontainerisasi adalah teknologi virtualisasi ringan yang memungkinkan aplikasi dan seluruh dependensinya dikemas dalam sebuah unit

terisolasi yang disebut *container*. Meningkatkan isolasi kontainer sangat penting dalam mencegah pelanggaran keamanan di lingkungan yang menggunakan kontainerisasi. Dengan memanfaatkan solusi keamanan kontainer, organisasi dapat memperkuat perlindungan terhadap ancaman dan kerentanan tingkat lanjut, sehingga secara signifikan mengurangi risiko terjadinya pelanggaran keamanan dalam sistem.

Arsitektur berbasis layanan yang dikontainerisasi memungkinkan pemanfaatan sumber daya yang lebih baik dan skalabilitas yang lebih tinggi. Skala, cakupan, dan dimensi yang dianalisis dalam penelitian ini berbeda dari pendekatan lain yang telah ditinjau. Kemampuan untuk membagi bagian-bagian dari suatu aplikasi dari satu menjadi banyak, lalu meningkatkan kapasitas tambahan pada host yang sama atau lainnya dalam lingkungan klaster seiring dengan perubahan permintaan tanpa intervensi manual, jauh lebih sesuai dengan lanskap digital yang terus berkembang saat ini. (Mulahuwaish dkk., 2022).

Untuk itu penulis membuat penelitian skripsi yang berjudul Perancangan Aplikasi Penyediaan Server Dengan Pengamanan Menggunakan Virtualisasi dan Kontainerisasi, harapnnya penelitian dapat meningkatkan tingkat keamanan dan integritas data pada server *multi-tenant*. Dengan meminimalkan risiko perpindahan serangan *antar-tenant*, diharapkan keamanan sistem dapat terjaga dengan lebih baik, sehingga melindungi data dan aplikasi dari ancaman siber.

1.2 Rumusan Masalah Penelitian

Beberapa permasalahan yang telah dipaparkan sebelumnya, Peneliti merumuskan beberapa rumusan masalah dalam penelitian ini di antaranya:

1. Bagaimana merancang arsitektur penyediaan server dengan pengamanan menggunakan virtualisasi dan kontainerisasi?
2. Bagaimana kemampuan arsitektur penyediaan server dengan pengamanan menggunakan virtualisasi dan kontainerisasi dari serangan siber?

1.3 Tujuan Penelitian

Adapun tujuan penelitian yang akan dicapai sebagau berikut:

1. Mengetahu dan merancang arsitektur penyediaan server dengan pengamanan menggunakan virtualisasi dan kontainerisasi.
2. Menguji kemampuan arsitektur penyediaan server dengan pengamanan menggunakan virtualisasi dan kontainerisasi dari serangan siber .

1.4 Batasan Penelitian

Agar penelitian lebih terfokus, batasan penelitian ini adalah:

1. Penelitian hanya berfokus pada pengukuran tiga jenis serangan sistem: RCE, Privilege Escalation, dan Sandbox Escape.
2. Setiap CVE yang akan diuji hanya diambil satu per-jalur serangan dan berdasarkan kerentanan terbaru.
3. Arsitektur yang dirancang menggunakan Proxmox untuk virtualisasi dan K3S untuk kontainerisasi.
4. Pengembangan dilakukan dalam lingkungan simulasi dengan skala terbatas yaitu hanya pada satu data center.
5. Pengembangan arsitektur tidak berupa UI yang dapat berinteraksi dengan pengguna, melainkan sebuah miniatur yang diimplementasikan kedalam perangkat Raspberry pi 4.
6. Orientasi sistem operasi yang digunakan pada penelitian ini hanya terbatas pada lingkungan sistem operasi linux.

1.5 Manfaat Penelitian

1.5.1 Manfaat Teoritis

Manfaat teoritis dari penelitian ini diantaranya:

1. Penelitian ini memberikan kontribusi dalam pengembangan arsitektur keamanan server yang lebih Tangguh.
2. Penelitian ini mengusulkan model isolasi baru yang menggabungkan virtualisasi (Proxmox) dan kontainerisasi (K3S) untuk meningkatkan keamanan antar *tenant*.
3. Hasil penelitian ini dapat menjadi dasar atau referensi bagi penelitian selanjutnya yang berkaitan dengan keamanan server multi-tenant, virtualisasi, dan containerisasi.
4. Penelitian ini membantu memahami mekanisme serangan siber dan cara meminimalisir dampaknya melalui pendekatan arsitektur yang tepat.

1.5.2 Manfaat Praktis

Adapun manfaat praktis dari penelitian ini yaitu:

1. Arsitektur yang dirancang dapat digunakan oleh penyedia layanan server untuk meningkatkan keamanan infrastruktur mereka, terutama dalam lingkungan *multi-tenant*.
2. Dengan implementasi arsitektur ini, dampak serangan dapat dibatasi, sehingga mengurangi risiko kerugian finansial dan reputasi.
3. Penelitian ini dapat digunakan sebagai bahan edukasi untuk meningkatkan kesadaran akan pentingnya keamanan server dan isolasi antar *tenant*.

1.6 Struktur Organisasi Skripsi

Penelitian ini ditulis dengan pedoman yang sebagian besar mengacu pada Pedoman Penulisan Karya Ilmiah Universitas Pendidikan Indonesia Tahun 2024. Sistematika penulisan penelitian ini adalah sebagai berikut:

1. PENDAHULUAN

Bagian Bab I ini memberikan penjelasan tentang latar belakang penelitian yang juga mencakup gap penelitian, rumusan masalah penelitian, tujuan penelitian, manfaat teoritis dan praktis, batasan masalah penelitian, hipotesis penelitian, dan struktur organisasi skripsi.

2. TINJAUAN PUSTAKA

Tinjauan Pustaka membahas mengenai studi literatur terkait penelitian. Beberapa bagian dalam bab ini menjelaskan tentang konsep, metode, teori, dan teknologi yang digunakan.

3. METODE PENELITIAN

Metode Penelitian membahas tentang prosedur penelitian. Ini mencakup jenis dan metode penelitian yang digunakan, perancangan desain arsitektur, perancangan jaringan, penentuan aturan *firewall*, dan teknik pengujian dan rencana analisis.

4. HASIL DAN PEMBAHASAN

Pada Bab IV Hasil dan Pembahasan akan memaparkan hasil yang diperoleh dari penelitian yang telah dilakukan, berupa analisis hasil pengujian isolasi jaringan, *firewall*, penyediaan *server*, dan hasil evaluasi tingkat kesulitan serangan.

5. SIMPULAN DAN SARAN

Bab terakhir, yaitu Simpulan dan Saran, merangkum temuan penelitian. Simpulan dari hasil penelitian disajikan, diikuti dengan pembahasan implikasi dari penggunaan arsitektur Proxmox dan K3S dalam meningkatkan keamanan *server multi-tenant*. Terakhir, penulis menyampaikan rekomendasi untuk pengembangan penelitian selanjutnya, memberikan arah bagi peneliti masa depan untuk mengembangkan konsep dan aplikasi lebih lanjut dalam bidang keamanan server, virtualisasi, dan kontainerisasi.