49/S/TEKKOM-KCBR/PK.03.08/24/JANUARI/2025

PERANCANGAN ARSITEKTUR PENYEDIAAN SERVER DENGAN PENGAMANAN MENGGUNAKAN VIRTUALISASI DAN KONTAINERISASI

SKRIPSI

diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana Teknik Komputer

Oleh

Fany Muhammad Fahmi Kamilah

NIM 2004339

PROGRAM STUDI S1 TEKNIK KOMPUTER

KAMPUS UPI DI CIBIRU

UNIVERSITAS PENDIDIKAN INDONESIA

2025

HALAMAN HAK CIPTA

PERANCANGAN ARSITEKTUR PENYEDIAAN SERVER DENGAN PENGAMANAN MENGGUNAKAN VIRTUALISASI DAN KONTAINERISASI

oleh

Fany Muhammad Fahmi Kamilah

NIM 2004339

Sebuah Skripsi yang Diajukan untuk Memenuhi Salah Satu Syarat Memperoleh Gelar Sarjana Teknik pada Program Studi S1 Teknik Komputer

Universitas Pendidikan Indonesia

Januari 2025

HALAMAN PENGESAHAN SKRIPSI

Fany Muhammad Fahmi Kamilah

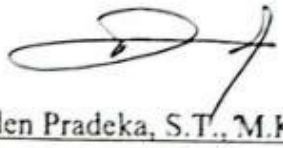
PERANCANGAN ARSITEKTUR PENYEDIAAN SERVER DENGAN PENGAMANAN MENGGUNAKAN VIRTUALISASI DAN KONTAINERISASI

disetujui dan disahkan oleh:

Pembimbing I

Dr. Eng. Munawir, S.Kom., M.T.
NIP. 920200819851205101

Pembimbing II



Deden Pradeka, S.T., M.Kom.
NIP. 920200419890816101

Mengetahui,
Ketua Program Studi Teknik Komputer

Deden Pradeka, S.T., M.Kom.
NIP. 920200419890816101

HALAMAN PERNYATAAN

KEASLIAN SKRIPSI DAN BEBAS PLAGIARISME

Dengan ini saya menyatakan bahwa skripsi dengan judul "Perancangan Arsitektur Penyediaan Server dengan Pengamanan Menggunakan Virtualisasi dan Kontainerisasi" ini beserta seluruh isinya adalah benar benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung resiko/sanksi apabila dikemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, Januari 2025

Yang membuat pernyataan

Fany Muhammad Fahmi Kamilah

NIM. 2004339

HALAMAN UCAPAN TERIMA KASIH

Segala puji dan syukur penulis haturkan kepada Allah SWT atas rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi berjudul "Perancangan Arsitektur Penyediaan Server dengan Pengamanan Menggunakan Virtualisasi dan Kontainerisasi". Penulisan skripsi ini bertujuan sebagai salah satu syarat kelulusan dalam sidang skripsi di Jurusan Teknik Komputer, Universitas Pendidikan Indonesia Kampus Cibiru.

Proses penelitian dan penulisan tidak lepas dari berbagai kendala. Namun, berkat dukungan, motivasi, dan bimbingan dari banyak pihak, penulis akhirnya mampu menyelesaikan karya ini. Dengan kerendahan hati, penulis mengucapkan terima kasih kepada:

1. Kedua orang tua tercinta beserta saudara yang senantiasa memberikan dukungan moril dan materil tanpa batas, serta doa tulus yang menjadi kekuatan penulis. Semoga Allah SWT senantiasa melimpahkan kesehatan dan kebahagiaan untuk mereka.
2. Bapak Dr. Eng. Munawir, S.Kom., M.T., selaku Dosen Pembimbing Pertama. Terima kasih atas kesabaran, waktu, dukungan mental, kritik konstruktif, dan perspektif mendalam yang bapak berikan, sehingga penelitian ini dapat berkembang secara metodologis dan akademis.
3. Bapak Deden Pradeka, S.T., M.Kom., selaku Ketua Program Studi Teknik Komputer dan Dosen Pembimbing Kedua. Terima kasih atas ilmu, bimbingan, serta kesabaran Bapak dalam mengarahkan penelitian ini hingga tuntas. Tanpa arahan dan masukan dari Bapak, pencapaian ini tidak akan mungkin terwujud.
4. Kawan kawan seperjuangan Aceng, Aduy, Ajay, Aldi, Ardi, Ce'i, Dean, Dorman, Icam, Jarwo, Uda, dan Wirwir yang telah membersamai dengan penuh semangat sehingga memberikan dorongan kuat untuk menyelesaikan

penelitian ini. Semoga bisa terus menjaga tali silaturahmi dan mencapai sukses bersama.

5. Rekan-rekan Teknik Komputer Angkatan 2020 terutama Dhimaz P., Ivan R., M. Radya, Rizal H., Rizal M. Terima kasih atas kebersamaan, semangat kolektif, dan momen berharga yang kita bagi. Keberhasilan ini adalah hasil dari perjalanan bersama, dan semoga ikatan kita tetap terjalin di masa depan.

Penulis menyadari sepenuhnya bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran dari pembaca sangat penulis harapkan untuk penyempurnaan karya ini. Semoga penelitian ini dapat memberikan manfaat, khususnya dalam pengembangan teknologi virtualisasi dan kontainerisasi di bidang keamanan server.

ABSTRAK

Perkembangan server multi-tenant menjadi tantangan kritis di era digital, terutama seiring meningkatnya kompleksitas ancaman siber seperti *Remote Code Execution (RCE*), *Privilege Escalation*, dan *Sandbox Escape*. Penelitian ini bertujuan merancang arsitektur server *multi-tenant* yang aman dengan menggabungkan pendekatan virtualisasi menggunakan Proxmox dan kontainerisasi berbasis K3S untuk meningkatkan isolasi sumber daya dan meminimalisir dampak serangan. Metode penelitian menggunakan pendekatan *Design and Development (D&D)* dengan tahapan analisis, desain arsitektur hybrid, dan pengujian melalui analisis serangan berbasis Attack Path Analysis. Hasil penelitian menunjukkan bahwa arsitektur hybrid ini berhasil menciptakan isolasi hierarkis melalui kombinasi lapisan *virtual machine (VM)* menggunakan Proxmox dan isolasi kontainer dengan K3S, diperkuat oleh segmentasi jaringan menggunakan VXLAN. Analisa serangan terstruktur mengungkapkan bahwa penyerang memerlukan minimal 7 tahap eksploitasi melintasi VM, kontainer, dan jaringan untuk memengaruhi tenant lain, karena terdapatnya pengamanan berlapis. Hasil dari *attack path analysis* ini menunjukan bahwa integrasi virtualisasi dan kontainerisasi dapat memberikan barimeter keamanan berlapis sehingga penyerang untuk dapat mencapai target atau sistem utama harus melakukan eksploitasi disetiap langkah dikarenakan adanya isolasi pada arsitektur yang diimplementasikan.

Kata Kunci: Keamanan Server, Virtualisasi, Kontainerisasi, Proxmox, K3S, RCE, VXLAN.

ABSTRACT

The development of multi-tenant servers is a critical challenge in the digital era, especially as the complexity of cyber threats such as Remote Code Execution (RCE), Privilege Escalation, and Sandbox Escape increases. This research aims to design a secure multi-tenant server architecture by combining virtualization approaches using Proxmox and K3S-based containerization to improve resource isolation and minimize the impact of attacks. The research method uses a Design and Development (D&D) approach with stages of analysis, hybrid architecture design, and testing through Attack Path Analysis-based attack analysis. The results show that this hybrid architecture successfully creates hierarchical isolation through a combination of virtual machine (VM) layers using Proxmox and container isolation with K3S, reinforced by network segmentation using VXLAN. Structured attack analysis revealed that an attacker requires a minimum of 7 stages of exploitation across VMs, containers, and networks to affect other tenants, due to the presence of layered security. The results of this attack path analysis show that the integration of virtualization and containerization can provide a layered security barimeter so that attackers to reach the target or main system must perform exploitation at each step due to the isolation of the implemented architecture.

Keywords: *Server Security, Virtualization, Containerization, Proxmox, K3S, RCE, VXLAN.*

DAFTAR ISI

HALAMAN HAK CIPTA i
HALAMAN PENGESAHAN SKRIPSI ii
HALAMAN PERNYATAAN iii
HALAMAN UCAPAN TERIMA KASIH iv
ABSTRAK vi
ABSTRACT vii
DAFTAR ISI viii
DAFTAR TABEL x
DAFTAR GAMBAR xi
DAFTAR LAMPIRAN xii
BAB I PENDAHULUAN 1
1.1 Latar Belakang Penelitian 1
1.2 Rumusan Masalah Penelitian 5
1.3 Tujuan Penelitian 5
1.4 Batasan Penelitian 6
1.5 Manfaat Penelitian 7
1.5.1 Manfaat Teoritis 7
1.5.2 Manfaat Praktis 7
1.6 Struktur Organisasi Skripsi 7
BAB II TINJAUAN PUSTAKA 9
2.1 Multitenancy 9
2.2 Penyediaan Server (*Server Provisioning*) 9
2.3 Virtualisasi 10
2.3.1 Proxmox 11
2.4 Kontainerisasi 11
2.4.1 Kubernetes (K8S) 12
2.4.2 K3S 12
2.5 Remote Code Execution (RCE) 12
2.6 Previlage Escalation 12

2.7 Sandbox Escape 13
2.8 Penelitian Terkait 13
BAB III METODE PENELITIAN 16
3.1 Desain Penelitian 16
3.2 Identifikasi Masalah (*Identify the problem*) 16
3.3 Mendeskripsikan Tujuan (*Describe the objectives*) 17
3.4 Desain dan Pengembangan Sistem (*Design & develop the artifact*) 19
3.4.1 Desain Arsitektur Sistem Proxmox 19
3.4.2 Desain Jaringan 20
3.4.3 Desain Aturan Firewall 21
3.5 Desain Uji Coba Sistem (*Test the artifact*) 23
3.5.1 Desain uji coba Black box testing 23
3.5.2 Desain uji coba *Attack Path Analysis* 25
3.6 Desain Evaluasi Hasil Uji (*Evaluate testing result*) 26
3.7 Mengkomunikasikan Hasil Uji (*Communicating the testing result*) 27
BAB IV HASIL DAN PEMBAHASAN 28
4.1 Hasil Pengembangan Arsitektur Sistem Proxmox 28
4.2 Hasil Implementasi Arsitektur Sistem K3S Sec 30
4.3 Hasil Aturan *Firewall* 31
4.4 Hasil Pengujian Black Box Testing 33
4.5 Hasil Pengujian Attack Path Analysis 34
BAB V SIMPULAN, DAN SARAN 36
5.1 Simpulan 36
5.2 Saran 36
DAFTAR PUSTAKA 38
LAMPIRAN 41

DAFTAR TABEL

Tabel 2. 1 Penelitian Terkait 14
Tabel 3. 1 Tabel rancangan pengujian pelarangan komunikasi 24
Tabel 3. 2 Tabel Rancangan Pengujian Keberhasilan Komunikasi..... 25
Tabel 4. 1 Tabel Hasil Uji Black-Box Testing..... 33

DAFTAR GAMBAR

Gambar 3 1 Prosedur penelitian model D&D (J. Ellis & Levy, 2010) 16
Gambar 3 2 Desain Arsitektur Sistem 19
Gambar 3 3 Desain Jaringan menggunakan VXLAN..... 21
Gambar 3 4 Jalur Serang (Attack Path) 26
Gambar 4. 1 Mini Computer Sebagai Server Fisik..... 28
Gambar 4. 2 Tampilan Dashboard Proxmox Beserta VM Didalamnya 29
Gambar 4. 3 Tampilan CLI Pada K3S-Server Untuk Kendali K3S Sec Cluster... 31
Gambar 4. 4 Hasil Implementasi Aturan Firewall sys. 31
Gambar 4. 5 Hasil Implementasi Aturan Firewall sec. 32
Gambar 4. 6 Hasil Implementasi Aturan Firewall pub. 32
Gambar 4. 7 Diagram Attack Path Analysis Pada Jalur pub..... 35
Gambar 4. 8 Diagram Attack Path Analysis Pada Jalur sec..... 35

DAFTAR LAMPIRAN

Lampiran 1 Daftar harga perangkat keras 41

DAFTAR PUSTAKA

Adhikari, S., & Baidya, S. (2024). *Cyber Security in Containerization Platforms: A Comparative Study of Security Challenges, Measures and Best Practices*. https://arxiv.org/pdf/2404.18082

Andrew Tanenbaum, & Bos, H. (2014). Modern Operating Systems 4th Edition. Dalam *International Journal of Modern Physics C* (Vol. 19, Nomor 3).

Burns, B., Grant, B., Oppenheimer, D., Brewer, E., & Wilkes, J. (2016). Borg, omega, and kubernetes. *Communications of the ACM*, *59*(5). https://doi.org/10.1145/2890784

Howard, M., Leblanc, D., & Viega, J. (2009). 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them. Dalam *Technology*.

J. Ellis, T., & Levy, Y. (2010). A Guide for Novice Researchers: Design and Development Research Methods. *Proceedings of the 2010 InSITE Conference*. https://doi.org/10.28945/1237

Maine Bahasa. (2023, November 1). *Keamanan Cloud Multi-Tenancy: Definisi & Praktik Terbaik*. eSecurity Planet.

Mark Dowd, J. M. J. S. (2006). *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*. Pearson Education.

Merkel, D. (2014). Docker: lightweight Linux containers for consistent development and deployment. Dalam *Linux Journal* (Vol. 2014, Nomor 239).

Microsoft. (2024). *Microsoft Digital Defense Report 2024*.

Mitnick, K. D., & Simon, W. L. (2003). The Art of Deception: Controlling the Human Element in Security. *BMJ: British Medical Journal*.

Mulahuwaish, A., Korbel, S., & Qolomany, B. (2022). Improving Datacenter Utilization Through Containerized Service-based Architecture. *Journal of Cloud Computing*, *11*(1). https://doi.org/10.1186/s13677-022-00319-0

Nurfauziah, H., & Jamaliyah, I. (2022). Perbandingan Metode Testing Antara Blackbox Dengan Whitebox Pada Sebuah Sistem Informasi. *Jurnal Visualika*, *8*(2).

Ochei, L. C., Bass, J. M., & Petrovski, A. (2018). Degrees of tenant isolation for cloud-hosted software services: a cross-case analysis. *Journal of Cloud Computing*, *7*(1). https://doi.org/10.1186/s13677-018-0121-8

Provos, N., Mavrommatis, P., Rajab, M. A., & Monrose, F. (2008). All your iFRAMEs point to us. *Proceedings of the 17th USENIX Security Symposium*.

Rancher Labs. (2025, Januari 20). *K3s: Lightweight Kubernetes*. Diakses pada 20 Januari 2025, dari https://k3s.io.

Richey. (2017). Design and Development Research: Methods, Strategies, and Issues. *BMC Public Health*, *5*(1).

Rosenblum, M., & Garfinkel, T. (2005). Virtual machine monitors: Current technology and future trends. *Computer*, *38*(5). https://doi.org/10.1109/MC.2005.176

Smith, J. E., & Nair, R. (2005). *Virtual Machines: Versatile Platforms for Systems and Processes*. Elsevier.

Sommerville, I. (2016). Software engineering (10th edition). Dalam *Pearson Education Limited*.

Stallings, W., Agboma, F., & Jelassi, S. T. A.-T. T.-. (2016). Foundations of modern networking : SDN, NFV, QoE, IoT, and Cloud LK - https://glos.on.worldcat.org/oclc/927715441. Dalam *Network* (Vol. 139, Nomor 3).

Stuttard, D., & Pintp, M. (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*. John Wiley & Sons.

Turnbull, J. (2014). The Docker Book: Containerization is the new virtualization. Dalam *Aging* (Vol. 7, Nomor 11).

Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security, Sixth Edition. Dalam *Cengage Learning*.

Wibisono Gunawan, A.G Gultom Rudy, & Mantoro Teddy. (2024). Strategi Peningkatan Kapabilitas Satuan Siber DISPAMSANAU Melalui Pemanfaatan Artificial Intelligence Pada Keamanan Siber Berdasarkan National Institute of Standards and Technology Cybersecurity Framework Version 1.1. *Jurnal Review Pendidikan dan Pengajaran*, *7*(1), 968–975.

Widarma, A., & Siregar, Y. H. (2019). Rancangan Teknologi Virtualisasi Untuk Optimalisasi Server Di Universitas Asahan. *CESS (Journal of Computer Engineering, System and Science)*, *4*(2), 313–319.

Wijayanto, D., Firdonsyah, A., Adhinata, F. D., & Jayadi, A. (2021). Rancang Bangung Private Server Menggunakan Platform Proxmox dengan Studi Kasus: PT.MKNT. *Journal ICTEE*, *2*(2). https://doi.org/10.33365/jictee.v2i2.1333